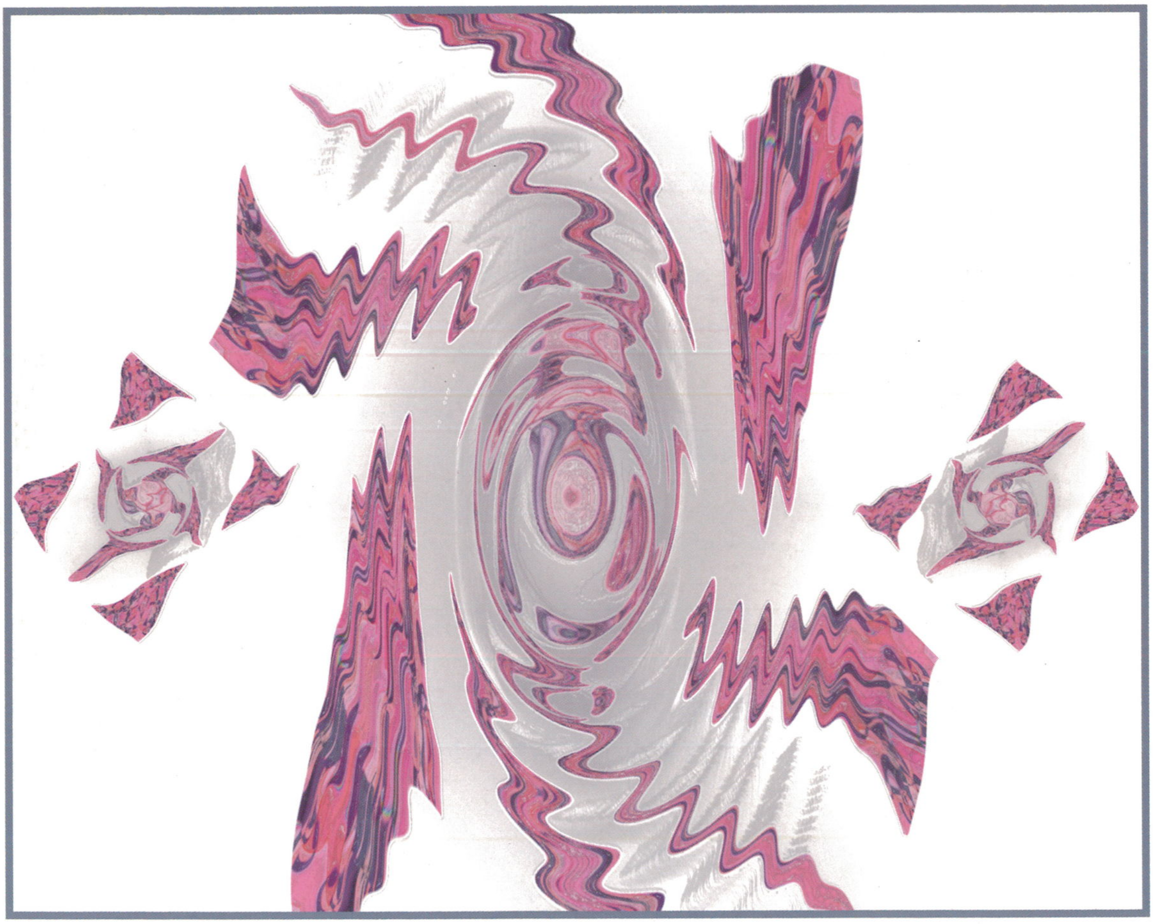
昭和38年7月2日第3種郵便物認可
2015年4月1日発行　第53巻4号　毎月1回1日発行
ISSN 0386—2240

数理科学

4
2015

特集 代数学における様々な発想
その思考方法の拡がりを知る



No.622
サイエンス社

幾何光学の正準理論

山本義隆 著　A5判・336頁・3900円(税別)

正準形式の幾何光学―そのシンプレクティック構造―を分かりやすく説明.変分原理としてのフェルマの原理の物理的意味を解明.

石取りゲームの数学 ―ゲームと代数の不思議な関係―

佐藤文広 著　A5判・256頁・3200円(税別)

石取りゲーム等, 必勝法を数学的に研究できる2人遊びゲームを題材に, ゲームの世界に潜む数学的構造の美しさ・深さを伝える.

● 数学の杜 2 ●

保型形式とユニタリ表現

髙瀬幸一 著　A5判・358頁・6000円(税別)

保型形式を記述するのに表現論がどのように関係するかを解説した入門書.

生誕100年 記念出版

小平邦彦―人と数学

【近刊】 3月中旬 刊行予定

20世紀数学界における巨人の一人である小平邦彦生誕100年記念出版. 小平博士自身による, 雑誌などに掲載された文章, 座談会などを収録.

また, 深い影響を受けた数学者による、その人となり, 思い出, そして, 小平数学の様々な角度からの解説を収めた.

日本数学会 編　A5判・約380頁・予価4600円(税別)

素数モンスター 新刊

―100までの数とそのキャラクターたち―



R.E.シュワルツ 著

下川理人・下川航也 訳

B5変型判・248頁・2000円(税別)

数学者が娘に素数と素因数分解を教えるために書いた算数・数学絵本.小学生から100歳まで楽しめる.

多面体 新装版

下川航也・平澤美可三・松本三郎・丸本嘉彦・村上 斉 訳

P.R.クロムウェル 著　B5変型判・448頁・4500円(税別)

ガロアに出会う ―はじめてのガロア理論―

のんびり数学研究会 著　A5判・192頁・2200円(税別)

● 数学書房選書 ●

桂 利行・栗原将人・堤 誉志雄・深谷賢治 編

4. 確率と乱数

杉田 洋 著　A5判・160頁・2000円(税別)

5. コンピュータ幾何

阿原一志 著　A5判・192頁・2100円(税別)

数学書房　101-0051 東京都千代田区神田神保町1-32-2 Tel 03-5281-1777 Fax 03-5281-1778
e-mail : mathmath@sugakushobo.co.jp　twitter:@sugakushobo

ガロア理論と表現論

ゼータ関数への出発



黒川信重／著

現代数学の基盤をなす《ガロア理論》と《表現論》のコンパクトな入門書。2つの理論を土台に、読者を《ゼータ関数論》へと促す。　●2,400円＋税

ピジョンの誘惑

論理力を鍛える70の扉



根上生也／著

すべての問題が、「鳩の巣原理」で解けるように工夫されたユニークな問題集。初級編から読み進むことで数学的思考を体得できる。　●1,500円＋税

線型代数［改訂版］ Linear Algebra

長谷川浩司／著

高校の学習指導要領改訂に伴い「0章：行列入門」を追加。2×2行列の基本から丁寧に解説。応用面も含め線型代数で学ぶべきことをほぼ網羅した、「教科書」を超えた一冊。　●3,300円＋税

数学史の小窓　中村 滋／著

いくつかの新発見により、近年大きく変わりつつある「数学史」を、黎明期から現代にかけて、やさしく紹介する。　●2,000円＋税

新しい解析入門コース［新装版］

堀川穎二／著

数学という広大な空間へ飛び立つために、土台となる《解析》の意味を明確に伝えたい。東大教養学部で使われた名教科書が復活!　●2,200円＋税

理系ジェネラリストへの手引き

岡村定矩・伊藤隆一・三浦孝夫・玉井哲雄／編著

理系の学部生に求められるリテラシーを一冊に収録。実験のレポート作成、統計処理、プレゼンなど、あらゆる場面で役立つ必携書。　●2,200円＋税

dxとdyの解析学［増補版］

高瀬正仁／著

積分に現われるdxと導関数の記号dxは同じなのか――を出発点にオイラーの言葉に耳を傾けながら進める名著。微分方程式の章を増補。　●2,800円＋税

数学セミナー ４月号　好評発売中

特集 **大学生に薦める数学の教科書**

大学ではどんな教科書で学ぶのだろう？ と不安に思っている新入生の皆さんや、もっと深く学びたい大学生の皆さんに向けて、ぜひ読んでほしい教科書・テキストを紹介します。奥深く興味深い数学の世界へと、本たちが導いてくれます。　●1,040円＋税

日本評論社　〒170-8474 東京都豊島区南大塚3-12-4 TEL : 03-3987-8621 http://www.nippyo.co.jp/

MATHEMATICAL SCIENCES
Number 622 April 2015

代数学における様々な発想

その思考方法の拡がりを知る

表紙：戸川 隼人

お得な定期購読をおすすめします

毎号確実に御手元へ

地域によって書店店頭に陳列されない場合があります．**郵送料小社負担**にて確実に御手元へ届く定期予約購読をおすすめします．

予約購読は１年間（本誌のみ）11,000 円，半年間（本誌のみ）5,500 円．（税込み価格）

造本コストは更に上昇気味です．小社としてもあらゆる努力をもって廉価で提供してゆきたいと思っておりますが，定価改定の止むなき事態がかんがえられます．この場合予約購読期間中のものにつきましては料金据置きとなります．なお，臨時別冊のご注文については，本誌予約購読者の方には，商品到着後のお支払いにて承ります．

お申し込みは本誌とじ込みの振替用紙を御利用下さい．

数理科学特集一覧

63 年/7～2011 年/12 省略

2012 年/1 数学から物理へ，物理から数学へ
/2 古典のススメ[物理編]
/3 量子を操る
/4 量子力学の数学的技法
/5 解析学と物理学
/6 面白い発想[物理編]
/7 数学と物理における格子
/8 導来圏をめぐって
/9 ハイゼンベルク
/10 超弦理論の数理
/11 物理と数学における厳密解
/12〈振動する〉物理

2013 年/1 表現論の世界
/2《量子化》の発想
/3 光と物理学
/4 解析学における様々な発想
/5 次元の作法
/6 発展する統計力学
/7 群と物理学
/8 エネルギーを通して物理学を知る
/9 ボーア
/10 分類する《数理科学》
/11 理論物理と実験物理の交錯
/12 物理学における存在とは

2014 年/1 波と粒子
/2 利用する物理
/3 幾何学における様々な発想
/4 物理現象における表現の多様さ
/5 数理科学における代数的構造
/6 数学と物理における空間概念
/7 モノポールの謎
/8 ベクトル解析の力
/9 重力の謎と魅力
/10 複素解析の視点
/11 応用するトポロジー
/12 場と力の物理イメージ

2015 年/1 科学における〈時間〉
/2 物理学諸分野の拡がりとつながり
/3 団代数をめぐって

数理科学臨時別冊一覧

14 年/8 情報幾何学の新展開
14 年/9 作用素環と無限量子系
14 年/10 重力とエントロピー
14 年/11 数学的な感覚の探求
14 年/12 4 次元微分幾何学への招待
15 年/1 ゲージ理論の基礎数理
15 年/3 ループ量子重力理論への招待

「数理科学」のバックナンバーは下記の書店・生協の自然科学書売場で特別販売しております

紀伊國屋書店本店（新宿）
紀伊國屋書店新宿南店
あおい書店中野本店
オリオン書房ノルテ店（立川）
くまざわ書店八王子店
くまざわ書店桜ヶ丘店（多摩）
書泉グランデ（神田）
三省堂本店（神田）
リブロ池袋店
ジュンク堂池袋本店
芳林堂（高田馬場）
MARUZEN & ジュンク堂渋谷店
八重洲ブックセンター（東京駅前）
丸善丸の内本店（東京駅前）
丸善日本橋店
MARUZEN 多摩センター店
ジュンク堂吉祥寺店
ブックファースト青葉台店（横浜）
有隣堂イセザキ町本店（横浜）
有隣堂西口・東口（横浜）
有隣堂厚木店（厚木）
ジュンク堂盛岡店
丸善津田沼店
ジュンク堂新潟店
ジュンク堂甲府岡島店
MARUZEN & ジュンク堂新静岡店
戸田書店静岡本店
ジュンク堂大阪本店
紀伊國屋書店梅田店（大阪）
アバンティブックセンター（京都）
ジュンク堂京都店
ジュンク堂三宮店
ジュンク堂三宮駅前店
ジュンク堂大分店
喜久屋書店倉敷店
MARUZEN 広島店
紀伊國屋書店福岡本店
ジュンク堂福岡店
丸善博多店
ジュンク堂鹿児島店
紀伊國屋書店新潟店
ジュンク堂旭川店
金港堂（仙台）
金港堂パーク店（仙台）
ジュンク堂秋田店
ジュンク堂郡山店
鹿島ブックセンター（いわき）
友朋堂（つくば）

――大学生協・売店――

東京大学 本郷・駒場
東京工業大学 大岡山・長津田
東京理科大学 新宿
早稲田大学 理工学部
慶応義塾大学 矢上台
福井大学
筑波大学 大学会館書籍部 第一学群書籍部
埼玉大学
名古屋工業大学・愛知教育大学
大阪大学・神戸大学 ランス
京都大学・九州工業大学
東北大学 理薬・工学
室蘭工業大学
徳島大学 常三島
愛媛大学 城北
山形大学 小白川
島根大学
学習院大学 成文堂
北海道大学 クラーク店
熊本大学
名古屋大学
広島大学（北１店）
九州大学（理系）

MATHEMATICAL SCIENCES
April 2015 Number 622

特集／代数学における様々な発想

代数の発想と進化

寺 杣 友 秀

1. 代数の起こり

数学の分野は大雑把にいって，代数，幾何，解析がある．しかし実際はこれらの分野が互いに交錯し合い，統合的に，あるいは独自の世界を形づくりながら発展している．「ここまでが代数」という境界ははっきりしていないものの，代数と呼ばれる分野の共通にある考え方は，数の体系に共通な四則演算などの構造を抽象化して，その計算方法を確立し，さらにもとに戻って応用するところにあるだろう．代数を意味するアルジェブラという言葉は，アラビアの数学者フワーリズミーの著書『ジェブルとムカーバラの算法の摘出』に語源をもち，数式の変形法と方程式を扱うものであった．中学生で学ぶ方程式は典型的な代数の問題である．未知数を x とおいて問題を x の方程式で表して，一般的に数について成り立つ計算法則を用いて x を求めるというものである．現代ではこういったものをさらに発展させ，統一的に扱うための枠組みと公理系が考えられている．代数の起源としてもう一つ見逃せないのは，エジプトのアレクサンドリアに住んでいたとされる，ディオファントスによる13巻に及ぶ著書『算術』であり，代数学の基礎を作ったとされている．方程式の整数解に関する問題も多く扱っており，フェルマーも彼の最終定理をこの本の余白に書き残したことは有名である．

2. 幾何との融合

幾何的対象を式で表して，その形式的変形により問題を系統的に扱う技法はデカルトの座標の導入に始まる．幾何の問題に代数が用いられるようになり，これは現在の代数幾何の出発点でもある．例えば円 C を考え，C の内部の中心ではない点 P をとる．P を通る直径でない直線 L は円と2点 $\mathrm{Q}_1, \mathrm{Q}_2$ で交わるが，そこでの円の接線の交点 R を考える．P を通る L を動かしたとき，R の軌跡は直線を動くことは，双対性として語られる有名な事実であるが，代数的には次のように示される．まず円 C が $x^2+y^2=1$ で表される座標をとり，$\mathrm{P}, \mathrm{Q}_1, \mathrm{Q}_2$ の座標を $(p_0, q_0), (p_1, q_1), (p_2, q_2)$ として，直線 L の方程式を $ax+by=1$ とする．$\mathrm{P}, \mathrm{Q}_1, \mathrm{Q}_2$ は直線 L 上にあるので，$ap_0+bq_0=ap_1+bq_1=ap_2+bq_2=1$ が成り立っている．また $\mathrm{Q}_1, \mathrm{Q}_2$ における円 C の接線はそれぞれ $p_1x+q_1y=1$, $p_2x+q_2y=1$ と表されるのでその交点 R の座標は (a,b) となる．ところが (a,b) は上の式から $p_0x+q_0y=1$ で定義される直線上にあることがわかる．このように幾何と代数を互いに関連づけることにより見通し

のよい理解が得られることは多い．

代数方程式の解法は２次方程式の平方根を用いた解法は，３次方程式，４次方程式の解法と進化したが，５次方程式の解法のところで一つの転機が訪れる．４次方程式まで，有効であった冪根による解法では不十分であるというガロアの発見である．ガロアの理論により，方程式の根の置換を出発点として群の概念が確立され，代数学の取り扱うことのできる対象が広がってきた．また力学や，連立１次方程式を取り扱う手段から発展してきたベクトルや行列を抽象化して扱う学問として線型代数学が起こり，数学全体とその応用分野に浸透していった．こうして現代代数学へと突入していく．

3. 現代の代数学

代数学に限ることではないが，現代数学の一つの特徴は公理的方法と抽象化にある．先ほど挙げた群の発想は方程式の解の置換に端を発するものであるが，その概念は幾何学にも影響を与えた．クラインは「エルランゲンの目録」の中で，幾何とは合同変換によって普遍な性質を研究であると，研究方向を明確化した．平面図形における合同変換群を別種の群に取り替えることにより双曲幾何，球面幾何などの別種の幾何が考え得るのである．さらに「群」を作用としてではなく，抽象的に扱う群論が現れ，表現論が現れた．群の他にも，環，体，リー群などの代数系が研究対象となり，それぞれの研究分野は，互いに関連しつつ発展してきた．

また相対性理論がローレンツ群による不変的な物理法則の探求から始まったように，現代数学は理論物理の考え方にも大きな影響を与えるようになってきた．現代物理では物理法則を表すのに群やリー群とその表現論は欠かすことのできない言葉となっている．

現代数学における抽象化の流れとあいまって，多様体の概念が確立され，市民権を得るようになると，位相幾何的手法を用いた多様体のコホモロジーなどの不変量の理論が確立されてくるようになった．その理論は代数分野にも大きな影響を与え，コホモロジー理論は圏論的な抽象化，一般化へと進んでいった．そういった抽象化を徹底的に推し進めていったのがグロタンディークで，圏と関手を基礎とした代数幾何の基礎付けが展開した．ヴェイユは有限体上の多様体に関するリーマン予想の類似としてヴェイユ予想を提出したが，これに触発されてグロタンディークはエタールコホモロジーの理論を展開し，整数論，代数幾何の分野をはじめ，ホッジ理論などの複素幾何学の分野にも大きな影響を与えた．「フェルマーの最終定理」のワイルズとテーラーによる解決は，代数幾何の基礎付けなしにはあり得なかった．こういった圏論的な扱いを前面に押出す考え方は群やリー群の表現論の分野にも大きな影響を与えた．無限次元表現の理論において，基本的な問題であったカジュダン・ルスティック予想の解決においても，交叉コホモロジー理論が使われた．その際，微分作用素の環とその上の加群の三角圏の言葉に言い換えるところが鍵となっていた．そこで使われた t-構造がフーリエ・向井変換などの定式化を通して，理論物理のミラー対称性に使われるとは誰が予想していただろうか？ 頂点作用素代数や無限次元リー群の表現において，理論物理的から出発した概念や手法が取り入れられるようになり，どこまでが代数なのかどころか，どこまでが数学なのか，という境界さえもはっきりしなくなりつつある．

また，現代代数学の発展と計算機の発展との相互作用も見逃すことはできない．格子理論に端を発する，コードの理論が誤り訂正符号としてCDに用いられているし，初等整数論や楕円曲線が暗号理論に応用されている．本誌でも紹介されているように，グレブナー基底の理論も計算機上でインプリメントされ，統計学と融合して，新しい分野を構築している．今後，代数学がいかにこれまでの代数学の枠を超えた広がりをもって発展していくか，目が離せない．

（てらそま・ともひで，東京大学大学院数理科学研究科）

「線形代数」は「代数」であるか？

海 老 原 円

…己は詩によって名を成そうと思いながら，進んで師に就いたり，求めて詩友と交って切磋琢磨に努めたりすることをしなかった．かといって，又，己は俗物の間に伍することも潔しとしなかった．共に，我が臆病な自尊心と，尊大な羞恥心との所為である．（中島 敦『山月記』より）

1.「線形な代数」って？

「線形代数」という言葉に筆者が初めて触れたのは，30 年あまり前のことである（当時は「線型代数」と書くのが一般的であったが，昨今は「線形」と綴ることのほうが多いので，ここでも「線形」という表記で統一することにする）．

線形代数の教科書を手にしたとき，まずその題名を奇異に感じたことを覚えている．**線形な代数とはこれいかに？** …意味不明の言葉にとまどいつつも，「もしかしたら，前代未聞の深遠な理論なのではないか」という期待をいだいたものである．

実際に頁をめくってみると，**直線や平面の方程式，ベクトル，行列，連立 1 次方程式，行列式，線形空間**（ベクトル空間）といった単語が並んでいる．「線形空間」は別としても，今まで勉強してきたことがらから全くかけ離れた題材を扱っているのではないことを知り，軽い失望とともに若干の安堵をおぼえた．と同時に，「これは代数なのであろうか？」という疑問が湧き上がってきた．「代数というより，むしろ幾何なのではないか．…いや，代数であると同時に幾何なのではないか」などと，とりとめのないことを考えたものである．

2. 線形代数の 2 つの顔

当時の筆者の感想は，さほど的外れなものではない．線形代数には確かに代数学的な側面と幾何学的な側面がある．

連立 1 次方程式の考察は，線形代数の中で非常に重要な位置をしめるが，そのような考察をするとき，我々は線形代数の代数的な側面に触れている．一方，空間内の直線や平面を取り扱ったり，ベクトルに行列をかける変換について考えたりするとき，我々は線形代数の幾何学的な側面を強く意識している．

代数的な側面からみれば，線形代数は**1 次式を扱う代数学**であり，幾何学的な側面を取り出せば，それは**まっすぐな図形を取り扱う幾何学**である．線形代数のこの 2 つの顔は表裏一体をなしており，いわば車の両輪である．

3. たすきがけのレトリック

そう考えてみると，「線形代数」という言葉は，なかなか味わい深いものである．

冒頭に中島敦の『山月記』を引用したが，その中の「**臆病な自尊心**」，「**尊大な羞恥心**」という 2

つの表現に注目していただきたい．これが「尊大な自尊心」や「臆病な羞恥心」であったら，よくある陳腐な表現に過ぎない．ところが，下の図のように，異質のものが，いわば「たすきがけ」の状態で結びついたとき，卓越した文学の香りが漂う．

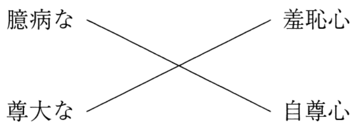


図 1　臆病な自尊心と尊大な羞恥心．

「線形」という言葉は，英語の「linear」の訳語であり，「まっすぐに伸びた」という意味である．この単語の持つ幾何学的な響きは，もとより「代数」とは異質のものである．

中島敦の流儀を借用するならば，線形代数は，**線形なる代数にして 1 次式の幾何**である．もし線形代数が「1 次式代数」という名前であったとしたら，我々はそこにどれほどのありがたみを感じるであろうか？ 1 次式代数？ ひょっとして，「3 日で振り返る中学数学」っていう手合いか？ 今さら何のつもりだ！ …また仮に，これが「線形幾何」であったとしても，どうもパンチが足りない．ところが….

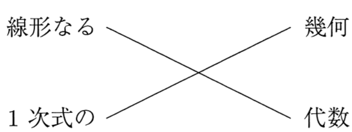


図 2　線形なる代数にして 1 次式の幾何．

線形なる代数にして 1 次式の幾何—何と文学的なレトリックであることか！

4. 連立 1 次方程式と行列の基本変形

次の連立 1 次方程式を考えよう．

$$\begin{cases} x + 2y = 7, \\ 2x + 5y = 16. \end{cases} \tag{1}$$

第 2 式から第 1 式の 2 倍を引くと $y = 2$ が得られるので，この方程式は簡単に解ける．まさしく「1 分で振り返る中学数学」である．

さて，この連立 1 次方程式にあらわれた係数や定数項を並べてみると

$$\begin{pmatrix} 1 & 2 & 7 \\ 2 & 5 & 16 \end{pmatrix} \tag{2}$$

となる．この行列を**拡大係数行列**とよぶ．ここで，第 2 式から第 1 式の 2 倍を引き，それを新たな第 2 式とする操作は，上の行列において第 2 行から第 1 行の 2 倍を引くという操作と対応する（行列の成分の横の並びを**行**という）．

$$\begin{pmatrix} 1 & 2 & 7 \\ 2 & 5 & 16 \end{pmatrix} \to \begin{pmatrix} 1 & 2 & 7 \\ 0 & 1 & 2 \end{pmatrix}. \tag{3}$$

このような操作は**行列の基本変形**とよばれる．

連立 1 次方程式を**消去法**によって解くことは，式変形を繰り返して**方程式を簡単にしていく**ことである．変形が終了した暁，我々は方程式に引導を渡す—「**お前はもう解けている！**」と．実際，上の例において，さらに新しい第 2 式（$y = 2$）の 2 倍を第 1 式から引けば

$$\begin{cases} x = 3, \\ y = 2 \end{cases} \tag{4}$$

という状態になる．すでにもう，**方程式なのか解なのか分からない状態**である．

そこで，線形代数においては，行列の基本変形を組織的に論ずる．

5. 1 次式から生ずるまっすぐな図形

線形代数は確かに 1 次式の代数学である．一方，1 次式は図形を定める．例えば

$$x + 2y + 3z = 0 \tag{5}$$

という式は空間内の平面を定める．実際

$$\boldsymbol{a} = \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} \tag{6}$$

がこの平面の**法線ベクトル**である．式 (5) は，原点 O と点 $\mathrm{P}(x, y, z)$ を結ぶベクトル $\overrightarrow{\mathrm{OP}}$ が $\boldsymbol{a}$ と直交することを意味するからである．

ところで，式 (5) を方程式とみて解くと，一般解は

$$x = -2\alpha - 3\beta, \quad y = \alpha, \quad z = \beta \tag{7}$$

（α, β は**任意定数**）と表されるが，これをベクトルの形に書き直せば

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \alpha \begin{pmatrix} -2 \\ 1 \\ 0 \end{pmatrix} + \beta \begin{pmatrix} -3 \\ 0 \\ 1 \end{pmatrix} \tag{8}$$

となる．式 (8) は，この方程式の表す平面上の点の位置ベクトルが，2 つのベクトルの**線形結合**（**1 次結合**）として表されることを意味する．これは平面の**次元**が 2 であるという事実につながる重要な考察である．

別の連立 1 次方程式を考えてみよう．

$$\begin{cases} x + 2y + 3z = 0, \\ x + y + 2z = 0, \\ 2x + 3y + 5z = 0. \end{cases} \tag{9}$$

この方程式の解をベクトルの形で表すと

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = t \begin{pmatrix} 1 \\ 1 \\ -1 \end{pmatrix} \tag{10}$$

（t は任意定数）となる．これは原点を通る直線を表す．任意定数が 1 個であるということは，直線が 1 次元であるという事実に対応する．

ところで，方程式 (9) は 3 本の式からなるが，第 3 式は第 1 式と第 2 式の和であるので，実質的には式 2 本分の効力しか持たない．一般に式の本数が多ければ，解の任意定数の個数は減る．しかし，今の例のように，単純に式の本数を数えるわけにはいかない．

方程式 (9) の係数のみを並べた行列（これを**係数行列**とよぶ）を A とすれば

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 1 & 2 \\ 2 & 3 & 5 \end{pmatrix} \tag{11}$$

である．行列 A は 3 本の**行ベクトル**（行列の行を横ベクトルと考えたもの）を含むが，第 3 行ベクトルは，第 1 行ベクトルと第 2 行ベクトルの**線形結合**（**1 次結合**）として表されている．一般に，あるベクトルが他のいくつかのベクトルの線形結合として表されるとき，それらは**線形従属**（**1 次従属**）であるという．また，そうでないとき，すなわち，どのベクトルも他のベクトルの線形結合として表せないとき，それらは**線形独立**（**1 次独立**）であるという．

ここで重要なのは，形式的に式が何本あるか，ということではなく，**実質的に式が何本分あるか**ということである．言い換えれば，**係数行列の行ベクトルのうち，線形独立なものがいくつあるか**，ということである．一般に，与えられた行列 A の行ベクトルのうち，線形独立なものの最大個数は A の**階数**（**ランク**）とよばれる．式 (11) の行列 A の階数は 2 である．

係数行列の階数は，いわば実質的な意味での式の本数であると考えることができ，それは，方程式の解の**自由度**，あるいは，対応する図形の次元と密接な関連がある．

6. 線形なる代数にして 1 次式の幾何

読者は，我々が代数学を論じているのか，幾何学を論じているのか，判然としなくなっていることにお気づきであろう．

人間の空間的感覚は非常に強力であるので，数学的考察において，それは頼りがいのある味方となる．一方，代数学の論理性は，考察を系統的に整理し，見通しをよくする．

このように，代数と幾何とが渾然と溶け合うところに線形代数の真骨頂がある．まさしく，線形なる代数にして 1 次式の幾何である．

7. 微分積分学にもあらわれる線形代数

大学の理工系の学部における数学の初年次教育においては，微分積分と線形代数が 2 本の柱である．しかし，これらは全く別のものというわけではなく，微分積分学にも線形代数の知識が必要である．例えば，2 変数関数 $f(x,y)$ の重積分において，変数変換

$$x = \varphi(u,v), \quad y = \psi(u,v) \tag{12}$$

を考えるとき，**ヤコビ行列式**

$$\det \begin{pmatrix} \partial\varphi/\partial u & \partial\varphi/\partial v \\ \partial\psi/\partial u & \partial\psi/\partial v \end{pmatrix} \tag{13}$$

が重要な役割を果たす．

一般に正方行列 A に対して**行列式** $\det A$（$|A|$ とも書かれる）が定まる．幾何学的にいえば，例えば 2 次正方行列 A の行列式は，平面図形に行列 A をかけたときの図形の**面積の拡大率**である．ただし，**図形が裏返ったときは，行列式は負であると**考える．

行列をかけることによって引き起こされる変換のイメージは次のようなものである．

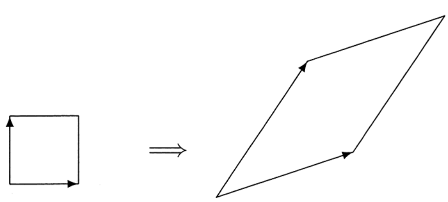


図 3　行列をかけると….

1 辺の長さが 1 の正方形に 2 次正方行列 A を作用させると，平行四辺形に変換される．そのときの面積の拡大率が $\det A$ である．

さて，積分とは何であろうか？ ある領域 D における関数 $f(x,y)$ の重積分を考えるときは，D を細かく分割し，**それぞれの部分の面積に，そのあたりでの f の値を乗じたもの**を求め，それらの総和をとる．そして，分割を細かくしていったときの極限を考える．—大まかにいえば，それが積分である．

ところで，変数変換 (12) を**微視的に見れば線形変換に非常に近い**．細かい領域に線形変換を施したときの面積の拡大率としてヤコビ行列式が自然に登場する，というわけである．

線形代数は，まっすぐな図形と 1 次式を扱う．しかし，まっすぐな図形と侮るなかれ．十分に滑らかな図形は，ミクロに見れば，ほぼまっすぐに見える．1 次式と侮るなかれ．十分に滑らかな関数は 1 次式近似を持つ．多くの場合，その近似を考察するだけでも，いろいろなことが分かる．

8. 一般化・抽象化

数学の理論は，しばしば一般化を志向する．

先ほど，連立 1 次方程式と空間内の図形と結びつけて考えた．3 つの未知数を持つ方程式の解集合は，空間内の図形をなす．ところが，連立 1 次方程式の未知数は 3 個に限らない．n 個の未知数を持ち，m 個の式からなる連立 1 次方程式の考察に呼応する形で，**n 次元ベクトル**という概念を導入するのが便利である．それには，n 個の数の組合せを考えればよい．

$$\boldsymbol{a} = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}. \tag{14}$$

一般に，平面ベクトルや空間ベクトルが与えられると，原点を始点としたときのそのベクトルの終点を考えることにより，ベクトルと平面（空間）内の点とが対応する．同様に，n 次元ベクトルを**点**と考え，n 次元ベクトル全体の集合を **n 次元空間**と考える．

また，複素数を成分とする複素ベクトルを考えたり，もっと一般に**体** K を与えて，K の元を成分とするベクトルを考えたりすることもできる（雑ないい方をすれば，体とは**四則演算**が運用できる体系のことである）．

ここで，「n 次元なんて，イメージがつかめない」と心配する向きもあるかもしれないが，そんな心

配は無用である．要するに n 個の数の組合せを考えるだけである．ただ，その組合せをあえて「ベクトル」とよぶのは，幾何学的な感覚を活かしたいからである．理論に幾何学的な彩りを加えることによって，空間的直観が躍動する舞台を作りたいからである．

9. 線形空間（ベクトル空間）—「線形代数」が「代数」となるとき

今まで漠然と「代数」という言葉を使ってきたが，現代的な意味での代数学は，いわば演算の構造論である．ある集合に演算が定まっているとき，「それがどういう集合であるか」，「演算の内容が何か」ということよりはむしろ，「その演算がどういう構造を持っているか」ということに着目するのが現代の代数学である．そういう意味において，線形代数が真に「代数」たり得るには，次に述べる**線形空間（ベクトル空間）**の導入を待たなければならない．

定義 1　空でない集合 V が体 K 上の線形空間（ベクトル空間）であるとは，$\boldsymbol{x}, \boldsymbol{y} \in V$ に対して $\boldsymbol{x}+\boldsymbol{y} \in V$ を対応させる演算と，$a \in K$, $\boldsymbol{x} \in V$ に対して $a\boldsymbol{x} \in V$ を対応させる演算とが定まり，次を満たすことである（ここで，$\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}$ は V の元を表し，a, b は K の元を表す）．

(1)　$(\boldsymbol{x}+\boldsymbol{y})+\boldsymbol{z}=\boldsymbol{x}+(\boldsymbol{y}+\boldsymbol{z})$.

(2)　$\boldsymbol{y}+\boldsymbol{x}=\boldsymbol{x}+\boldsymbol{y}$.

(3)　ある $\boldsymbol{0} \in V$ が存在して，任意の $\boldsymbol{x} \in V$ に対して $\boldsymbol{x}+\boldsymbol{0}=\boldsymbol{x}$ を満たす．

(4)　任意の $\boldsymbol{x}$ に対して $-\boldsymbol{x} \in V$ が存在して $\boldsymbol{x}+(-\boldsymbol{x})=\boldsymbol{0}$ を満たす．

(5)　$a(\boldsymbol{x}+\boldsymbol{y})=a\boldsymbol{x}+a\boldsymbol{y}$.

(6)　$(a+b)\boldsymbol{x}=a\boldsymbol{x}+b\boldsymbol{x}$.

(7)　$a(b\boldsymbol{x})=(ab)\boldsymbol{x}$.

(8)　$1 \cdot \boldsymbol{x}=\boldsymbol{x}$.

K の元を成分に持つ n 次元ベクトル全体を K^n と表す．K^n は K 上の線形空間である．したがっ

て，線形空間は K^n の一般化であると考えられるが，上の定義にしたがえば，さらにいろいろなものが線形空間となり得る．

線形空間は，理工系の学部学生がおそらく最初に触れる代数系であり，その抽象性にとまどう者も多い．

抽象化とは，物事の本質をできるだけ純粋な形で取り出す作業である．もちろん，その過程で切り捨てられるものもある．抽象化は，余分なものをできる限りそぎ落とすことによって，本質を浮き彫りにする—いわば**概念の断捨離**とでもいうべき作業である．例えば線形空間という概念は，ベクトルの**加法**，**スカラー乗法**という 2 つの演算の構造にのみ着目して，その本質を取り出したものであるので，例えばベクトルの**長さ（ノルム）**や**内積**といった概念は，ここでは捨てられている．

K が実数全体あるいは複素数全体の集合であるとき，**内積の入った線形空間**も考えることができ，それは**計量線形空間**などとよばれる（その定義はここでは割愛する）．

定義 2　K 上の 2 つの線形空間 V, V' に対して，写像 $T : V \to V'$ が次の 2 つの条件を満たすとき，T は K 上の**線形写像**であるという（ここで $\boldsymbol{x}, \boldsymbol{y}$ は V の元を表し，a は K の元を表す）．

(1)　$T(\boldsymbol{x}+\boldsymbol{y}) = T(\boldsymbol{x}) + T(\boldsymbol{y})$.

(2)　$T(a\boldsymbol{x}) = aT(\boldsymbol{x})$.

また，線形写像 $T : V \to V'$ が全単射であるとき，T は**同型写像**であるという．V から V' への同型写像が存在するとき，V と V' は**同型**であるという．

ベクトルに行列をかけて新たなベクトルを得るという操作を K^n から K^m への写像としてとらえると，これは線形写像である．したがって，線形写像は「行列をかける」という作用の一般化であると考えられる．

V と V' が同型であるとき，V と V' の間には，演算を含めた一対一の対応がつく．このとき，V と V' の線形空間としての構造は同一であると考えられる．

10. 基底と次元—座標の導入

かくして「線形代数」は現代的な意味において「代数」となった．もちろん，だからといって，幾何学であることを放棄したわけではない．そのことは，線形**空間**（ベクトル**空間**）という用語が用いられていることからも見てとれる．一般に，我々が**空間**とよぶところのものは，単なる集合ではなく，その集合に何らかの構造を付与し，そこに幾何学的な意味合いを付託したものである．

さて，平面ベクトルや空間ベクトルを取り扱う際に，**座標**を設定することによって**成分表示**できるようになったという点に注目しよう．同様のことをここでも考えたい．

定義 3　K 上の線形空間 V に対して，V の元の組 $\boldsymbol{e}_1, \boldsymbol{e}_2, \cdots, \boldsymbol{e}_n$ が次の 2 つの条件を満たすとき，これらは V の**基底**であるという．

(1)　$\boldsymbol{e}_1, \boldsymbol{e}_2, \cdots, \boldsymbol{e}_n$ は**線形独立**（1 次独立）である．

(2)　V は $\boldsymbol{e}_1, \boldsymbol{e}_2, \cdots, \boldsymbol{e}_n$ で**張られる**（**生成される**）．すなわち，V の任意の元がこれらの**線形結合**として表される．

ここで，線形結合（1 次結合），線形独立（1 次独立）といった概念は，通常のベクトルの場合と同様に定義される．

ここでは，有限個の元からなる基底について述べたが，無限個の元からなる基底の概念も定義することができる．集合論における**ツォルンの補題**を用いれば，線形空間は必ず基底を持つことが示される．

線形空間 V が有限個の元からなる基底を持つとき，V は**有限次元**であるといい，そうでないときは**無限次元**であるという．また，V の基底が n 個（$n < \infty$）の元からなるとき，V は n 次元であるという（この定義が **well-defined** であること，すなわち，いかなる基底も一定個数の元から

なることが知られている).

ここでは有限次元（その次元を n とする）の線形空間 V について考える．$\boldsymbol{e}_1, \boldsymbol{e}_2, \cdots, \boldsymbol{e}_n$ が基底であるとき，次のような写像 $\psi : K^n \to V$ を考えることができる．

$$K^n \ni \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \mapsto \sum_{i=1}^{n} x_i \boldsymbol{e}_i \in V. \qquad (15)$$

この写像は実は同型写像である．

この写像は，V 上の点とその座標とを対応させる写像にほかならない．例えば $n = 2$ の場合，$\boldsymbol{e}_1, \boldsymbol{e}_2$ が V の基底であるならば，$-2\boldsymbol{e}_1 + \boldsymbol{e}_2$ が $\begin{pmatrix} -2 \\ 1 \end{pmatrix}$ と対応する．

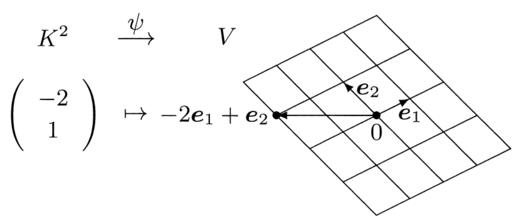


図 4　基底が定まれば座標が定まる．

フェルマやデカルトによって座標の考え方が導入されて以来の**解析幾何学**の系譜がここにも受け継がれていることに注目されたい．

このように，座標を入れることによって，我々は V の元を通常のベクトルのように見立てて取り扱うことができる．

線形写像についても考えてみよう．線形空間 V が基底 $\boldsymbol{e}_1, \cdots, \boldsymbol{e}_n$ を持ち，線形空間 V' が基底 $\boldsymbol{e}'_1, \cdots, \boldsymbol{e}'_m$ を持つとする．線形写像 $T : V \to V'$ に対して

$$T(\boldsymbol{e}_j) = \sum_{i=1}^{m} a_{ij} \boldsymbol{e}'_i \quad (1 \leq j \leq n) \qquad (16)$$

を満たす $a_{ij} \in K$ を用いて (m, n) 型行列 $A = (a_{ij})$ を作ることができる．この行列 A は T の**表現行列**とよばれる．読んで字の如く，線形写像が行列によって表現される．

座標を入れることによって，V の元をベクトルのように扱うことができ，線形写像をあたかも「行列をかける作用」のように見立てることができる．抽象化に伴って切り捨てたはずのベクトルや行列が，ここに復権をとげるのである．

11. 固有値と固有ベクトル，対角化とジョルダン標準形

もちろん，**基底を取りかえれば表現行列は変わる**．基底・座標はうまく選びたい．目的に応じてよりよい座標を選ぶことによって，物事はすっきりと理解できるはずである．

V から V 自身への線形写像（線形変換）T に対して，$\alpha \in K, \boldsymbol{x} \in V$ が

$$T(\boldsymbol{x}) = \alpha \boldsymbol{x}, \quad \boldsymbol{x} \neq \boldsymbol{0} \qquad (17)$$

を満たすとする．このとき，α を T の**固有値**とよび，$\boldsymbol{x}$ を**固有ベクトル**とよぶ．もし固有ベクトルだけからなる V の基底がとれれば，その基底に関する T の表現行列は**対角行列**となる．これがいわゆる**対角化**である．

対角化はいつでも可能であるとは限らないが，複素線形空間の線形変換に関しては，基底をうまく選ぶことによって，表現行列を**ジョルダン標準形**とよばれるものにすることができることが知られている．

こうしたことは，いずれも，**座標をうまく選ぶことによって，与えられた線形変換の幾何学的な本質を端的に表すような表現行列を見つける**という考え方に沿ったものである．

12. 線形代数の応用—上善は水のごとし

線形代数の応用範囲は広い．

例えば，ある区間上定義された滑らかな関数全体は，無限次元線形空間をなす．このように，関数全体を線形空間ととらえる考え方は，**関数解析**という分野につながる．関数解析学においては，関

数をベクトルのように見立てることによって，線形代数学的な手法を駆使した理論が構築される．

また，代数学において，**体の拡大**に関する理論がある．体 K を拡大して新たな体 L を作ったとき，L は K 上の線形空間とみることができる．そのようにみたときの L の次元を**体の拡大次数**とよび，$[L:K]$ と表す．

この稿では詳しく解説することができないが，体の拡大次数を身近に感じることのできる例として，ここでは**複素平面**を取り上げたい．実数全体の集合 $\mathbf{R}$ は体をなす（これを**実数体**とよぶ）が，それを含む体として複素数体 $\mathbf{C}$（複素数全体の集合のなす体）がある．したがって，$\mathbf{C}$ は $\mathbf{R}$ の**拡大体**であり，その拡大次数は 2 である．実際，複素数を指定するには，実部と虚部を指定すればよい．したがって，平面上の点と複素数とを対応させることができる．これが複素平面の考え方であるが，まさしくその次元は 2 である（**平面**であるので，当然であろう）．

さて，3 **大作図不可能問題**の中に**倍積作図問題**（別名：**デロスの問題**）というものがある．「与えられた長さを 1 辺にもつ立方体の 2 倍の体積を持つ立方体の 1 辺の長さを，定規とコンパスを用いて作図せよ」という問題であるが，それが不可能であることを，体の拡大次数を効果的に用いて証明することができる．

そのほかにも，**誤り訂正符号理論**というものには，有限体上の線形空間の理論が使われる．

このように，線形代数の応用は数多く存在し，それをいちいち取り上げることはできない．何しろ，線形代数は，線形なる代数にして 1 次式の幾何であるから，数学そのものに限らず，広く数理的思考が求められる場面で頻繁に顔を出すのは当然のことであろう．

「上善は水のごとし」（『老子』）という言葉がある．水の如く，それは様々な局面に入り込み，空気の如く，我々はそれを呼吸する．数学的思考において，我々はもはや，線形代数なしに済ますことはできないのである．

（えびはら・まどか，埼玉大学大学院理工学研究科）

代数方程式の天才たち



木村　俊一

1. 古代バビロニアの 2 次方程式

代数方程式の話が楽しいのは，幾多の天才たちがそれぞれの持ち味を発揮して大活躍するからであろう．その名場面をいくつかご紹介する．まずは紀元前の，名前も忘れ去られた天才の業績から．紀元前 18 世紀，ハンムラビ王の時代．次のような練習問題が，楔形文字で残されている．

> 正方形の面積から，正方形の一辺の長さを引いたら 870 になった．正方形の一辺の長さを求めよ．

4 千年近くも前に，2 次方程式だ．そしてその解答が，また格調高い．辺の長さの 1 倍を引いているので，その 1 の半分，つまり 0.5 を 2 乗して，0.25，これを 870 に加えて 870.25，この平方根を取ると 29.5 になる．さきほどの 0.5 を足して，$29.5 + 0.5 = 30$ が一辺の長さとなる．

$$x^2 - bx = c$$

という方程式が，

$$\frac{b}{2} + \sqrt{\left(\frac{b}{2}\right)^2 + c}$$

という解の公式で解ける，というわけである．

こんな 2 次方程式が解けても，この時代じゃ使い道がなかったろうに，よくぞこんな問題，そしてこんな解法を思い付いたものだ．いや，実はこれは実用的な問題が背景にある，という説がある．「面積は，その周の長さを測ることで測定することができる」という迷信があった，というのだ．もちろんそれは間違いだ．例えば周の長さが同じ長方形の形の土地であれば，正方形の場合が面積最大だ．一辺 t の正方形と周の長さが同じで，長辺と短辺の長さの差が b という長方形があれば，その長方形の面積

$$c = \left(t + \frac{b}{2}\right)\left(t - \frac{b}{2}\right) = t^2 - \left(\frac{b}{2}\right)^2$$

は正方形の面積 t^2 より $\left(\frac{b}{2}\right)^2$ だけ少ない．よって長方形の面積 c に $\left(\frac{b}{2}\right)^2$ だけ加えたものが正方形の面積 t^2 になり，よってその平方根が t だとわかる．したがって長辺の長さは $\frac{b}{2} + \sqrt{\left(\frac{b}{2}\right)^2 + c}$ として求められる，というわけである．この頃の数学者がこの知識を使って悪徳に儲けていたのか不正を糾弾していたのかはわからないが，この計算は要するに平方完成だ．人類は「目には目を，歯には歯を」の時代に既に，「2 次方程式には**平方完成**を」という知恵を持っていたのである．

2. タルタリアの 3 次方程式

さて，3 千年ほど時代がとんで，16 世紀のイタリアを見てみよう．ユークリッドに代表される「古代数学」では特別な場合を除いて解けない，とされてきた 3 次方程式が，実は解けるのではないかという噂が流れていた．この時代，新しい発見をし

ても，論文で発表したりはしない．数学勝負をしてライバルの問題を解いてみせることで，名声を勝ち取るのである．1535年，独学の数学家庭教師タルタリアと，名門ボローニャ大学で数学を学んだフィオルとの数学勝負において，双方3次方程式の問題を30問ずつ出し合い，30対0でタルタリアが圧勝した．3次方程式の解法を学ぼうとタルタリアのもとへイタリア中から数学者が集まってくるが，タルタリアは秘法を誰にも教えようとしない．皆さんには特別に3次方程式を解く秘法をお知らせしよう．

$$x^3 + px + q = 0$$

というパターンの3次方程式を考える．まず $(x+y+z)(x^2+y^2+z^2-xy-yz-zx)$ という式を展開すると

$$x^3 + y^3 + z^3 - 3xyz$$

となる．そこで

$$\begin{cases} y^3 + z^3 = q, & (1) \\ -3yz = p & (2) \end{cases}$$

という連立方程式が成り立つように y と z を選ぶことができれば，与えられた方程式が

$$x^3 + px + q = x^3 + y^3 + z^3 - 3xyz$$

と変形できるので，$x = -y - z$ が解になる，という仕組みである．上記連立方程式は，$Y = y^3, Z = z^3$ とおけば，

$$\begin{cases} Y + Z = q, & (3) \\ -27YZ = p^3 & (4) \end{cases}$$

となるので，2次方程式 $T^2 - qT - \frac{p^3}{27} = 0$ の2根 $\frac{q \pm \sqrt{q^2+4p^3/27}}{2}$ が Y と Z だ．y と z はそれぞれの3乗根だったので，解の公式

$$\sqrt[3]{\frac{-q+\sqrt{q^2+4p^3/27}}{2}} + \sqrt[3]{\frac{-q-\sqrt{q^2+4p^3/27}}{2}}$$

が得られた．

3. カルダノの3次方程式

タルタリアから秘法を聞き出した数学者がいた．1539年にカルダノが「神に誓って絶対に公表しない」という約束のもとで，3次方程式の解法を教えてもらったのである．ところがカルダノは1545年に『大いなる技法』という著書で3次方程式の解法を発表してしまった．怒り狂ったタルタリアはカルダノを非難するが，カルダノは相手にしない．後世には著書だけが残り，3次方程式の解法はカルダノの公式と呼ばれるようになった…，と昔何かの本で読んだのだが，事実は微妙に違うようだ．3次方程式の解法をどうしても発表したくなったカルダノは，ボローニャ大学を訪れてフィオルの師匠デル・フェッロの論文を調べ，既にそこに公式が記されていることを確かめたのである．そして，「絶対に公表しない」と約束したはずの解法をカルダノが発表したくなったのには，理由があった．カルダノは，タルアリアの解の公式に一工夫加えて，どんな3次方程式でも解けるようにしたのである．

タルタリアが必勝法を与えた3次方程式には2次の項がなかったことに気付かれただろうか？ 一般の $x^3+ax^2+bx+c=0$ というパターンの3次方程式だと，このパターンにあてはまらない．ところが $t = x + \frac{a}{3}$ と変数変換してみると，t^2 の項がキャンセルして

$$t^3 + \left(b - \frac{a^2}{3}\right)t + \left(\frac{2a^3}{27} - \frac{ab}{3} + c\right) = 0$$

という形になり，タルタリアの公式が使えるようになるのである．負の数がまだ一般的ではなかったこの時代，カルダノは3次方程式を係数の符号に従って何通りにも場合分けし，それぞれの場合で解法を紹介し，例題を解いて見せ，誰でもマニュアルに従って3次方程式を解けるように解説したのである．

一般に，$x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = 0$ という形の方程式は，$x = t + \frac{a_{n-1}}{n}$ と変数変換することで，x^{n-1} の係数を消すことができる．このような変換を，**カルダノ変換**と呼ぶ．2次方程式に対しては，カルダノ変換は平方完成に他ならない．3次方程式に対して立法完成はできないけれども，カルダノ変換がその一般化になっているのである．

4. フェラーリの 4 次方程式

カルダノの『大いなる技法』には，カルダノの弟子，フェラーリが発見したという 4 次方程式の解法も紹介されている．まず，カルダノ変換で 3 次の項を消して，

$$x^4 + ax^2 + bx + c = 0$$

という形にしたところから始めよう．アイデアは，適当に移項して，両辺とも完全平方になるようにしよう，ということである．例えば左辺が $x^4 + 2kx^2 + k^2$ という形になるようにすると（k の値はあとで決めることにする），元の方程式は

$$x^4 + 2kx^2 + k^2 = (2k - a)x^2 - bx + (k^2 - c)$$

と変形される．左辺 $= (x^2 + k)^2$ は既に完全平方なので，右辺も完全平方になるように k の値を選ぶことにしよう．2 次式として判別式が 0 になれば良いので，

$$b^2 - 4(2k - a)(k^2 - c) = 0$$

が成り立つように k を定めれば良い．これは k についての 3 次方程式なので，もう解き方はわかっている，というわけだ．解 k を求めて代入すると右辺が $(\alpha x + \beta)^2$ という形になるので

$$\begin{aligned}&(x^2 + k)^2 - (\alpha x + \beta)^2 \\ &= (x^2 + \alpha x + \beta + k)(x^2 - \alpha x + k - \beta) = 0\end{aligned}$$

と 2 次式の積に因数分解できて，元の 4 次方程式が解けることになる．

5. ボンベリの複素数

これで 4 次方程式までなら四則演算と冪根を使って，方程式を自由に解けるように見えるが，よく見ると話はそれほど単純ではない．例えば 3 次方程式

$$x^3 - 15x - 4 = 0$$

をタルタリアの解の公式で解こうとすると

$$\sqrt[3]{2 + 11\sqrt{-1}} + \sqrt[3]{2 - 11\sqrt{-1}}$$

となり，**複素数の 3 乗根**がでてきてしまう．ところが，$x = 4$ を代入してみると，確かに解になっていることが確かめられる．これは一体どうしたことか，4 という解はどこへ行ってしまったのか？これに対して，

> $(2 \pm \sqrt{-1})^3 = 2 \pm 11\sqrt{-1}$ だから，$2 \pm \sqrt{-1}$ をそれぞれの 3 乗根として
>
> $$(2 + \sqrt{-1}) + (2 - \sqrt{-1}) = 4$$
>
> と解が求まる

と観察したのが，16 世紀のボンベリである．実数係数の方程式で，解も実数なのに，複素数の 3 乗根が必要になってくるのである．方程式を解きたい，という目標からすると，これは結構深刻な問題だ．

深刻だという第 1 の理由は，複素数の 3 乗根が解の公式に現れるのが，例外的なケースに限らないことである．カルダノは方程式の様々なパターンに対して例題で解き方を紹介しているが，複素数の 3 乗根が出てくるケースは注意深く避けている．例外的ではないという証拠に，方程式 $x^3+px+q=0$ が相異なる 3 実根を持つための条件を調べてみよう．$p < 0$ のとき関数 $f(x) = x^3 + px + q$ は $x = \pm\sqrt{-\frac{p}{3}}$ で極大極小値をとり，そこでの f の値 $f(\pm\sqrt{-\frac{p}{3}}) = q \pm \frac{2p}{3}\sqrt{-\frac{p}{3}}$ の積は $q^2 + \frac{4p^3}{27}$ になる．$p \geq 0$ だとこれは決して負にならないこととあわせて，$q^2 + \frac{4p^3}{27} < 0$ が，3 次方程式 $x^3+px+q=0$ が相異なる 3 実数根をもつための必要十分条件だということがわかるが，$q^2 + \frac{4p^3}{27}$ はまさにタルタリアの解の公式のルートの中身だ！つまり，方程式が 3 つの相異なる実数解を持つ場合は常に（そしてそのときに限り），解の公式に複素数の 3 乗根が登場するのである．そもそもタルタリアの公式では解が 1 つしか出てこないので，実数解が 3 つあったら困ってしまうのだ．

ボンベリが解いた $x^3 - 15x - 4 = 0$ でも実数解があと 2 つあるはずだが，それを探してみよ

う．$\omega=\frac{-1+\sqrt{-3}}{2}$ とおくと，よく知られているように ω と ω^2 は 1 の 3 乗根であり，3 乗して $2+11\sqrt{-1}$ になる数としては $2+\sqrt{-1}$ の他に $(2+\sqrt{-1})\omega$ と $(2+\sqrt{-1})\omega^2$ が出てくることになる．3 乗根の取り方が 3 通りあるので，タルタリアの解の公式からは解が 9 つ出てきそうだが，連立方程式 (1), (2) を (3), (4) に帰着させたところをよく読み返してみると，$\sqrt[3]{Y}=y, \sqrt[3]{Z}=z$ は自由に選べるわけではなく，式 (2) を満たすように，すなわち 2 つの 3 乗根の積が $-\frac{p}{3}$ になるように選ばなくてはならない，ということがわかる．それを踏まえて，あと 2 つの解は

$$(2+\sqrt{-1})\omega+(2-\sqrt{-1})\omega^2=-2-\sqrt{3},$$
$$(2+\sqrt{-1})\omega^2+(2-\sqrt{-1})\omega=-2+\sqrt{3}$$

となり，タルタリアの公式からすべての解が導かれることがわかる．

第 2 の理由は，より深刻である．$x=2\cos 40^\circ$ の値を求めるためにタルタリアの公式を使ってみよう．3 倍角の公式 $4\cos^3\theta-3\cos\theta=\cos 3\theta$ において $\theta=40^\circ$ とおくと $x^3-3x+1=0$ という 3 次方程式が導かれるので，$\cos 40^\circ$ が四則演算と冪根で表せそうに見える．タルタリアの公式で解くと

$$x=\sqrt[3]{\frac{-1+\sqrt{-3}}{2}}+\sqrt[3]{\frac{-1-\sqrt{-3}}{2}}$$

となる．3 乗根の中身は，ω と ω^2 だ．絶対値が 1 の複素数 $\exp(i\theta)$ の 3 乗根は，ド・モアブルの公式を使って $\exp\left(\frac{i\theta}{3}\right)$ と求められる．$\omega=\exp\left(\frac{2\pi i}{3}\right)$ なので，

$$\sqrt[3]{\omega}=\exp\left(\frac{2\pi}{9}\right)=\cos 40^\circ+i\sin 40^\circ$$

である．同様に $\sqrt[3]{\omega^2}=\cos 40^\circ-i\sin 40^\circ$ なので $x=2\cos 40^\circ$ と解が求まった．…って，これでは意味がない．

n 乗根と言うと，正の実数 R に対して $\sqrt[n]{R}$ という正の実数を返す関数を何となく想定しているが，複素数の n 乗根を計算しようとすると，その他に角度の n 等分，という問題もからんでくるのだ．3 次方程式の場合で言うと，実数の関数として，$R>0$ に対して $\sqrt[3]{R}$ を返す関数の他に，$\cos 3\theta$ の値を入力すると $\cos\theta$ の値を返してくれるような「角の 3 等分関数」も必要なのである（ちなみに，2 次方程式までは実数の平方根だけですべて計算できる）．複素数が市民権を得るのが 1800 年頃，複素平面が発明されて複素数が「可視化」された時期であった．複素数がもたらす問題点が曖昧な段階で，先に「方程式の冪根による解法」の研究が，これからお話するように進んだのは，ある意味ラッキーだったかもしれない．いや，もちろん「正の実数の n 乗根と角度の n 等分という関数を使って解を書き下す問題を解決したのだ」，と表現すれば，問題点でも何でもないのだけれども，問題の響きの格調がかなり失われているように感じられるのである．

6. ラグランジュの置換（2 次方程式）

フェラーリのあと，5 次方程式の解の公式を求めて様々な研究がなされたが，なかなか公式は見つからない．解の公式はなさそうだ，という感触がそろそろつかめてきていたのではないだろうか？ その「感触」を数学の言葉で最初に表現したのが，ラグランジュであった．方程式の解ひとつひとつを求めようとするのではなく，解全体をいっせいに考えて，その間の**置換**を考察しよう，というのである．まず 2 次方程式の場合に見てみよう．

2 次方程式 $x^2+ax+b=0$ の 2 つの解を α,β とすると，解と係数の関係により，

$$\begin{cases}\alpha+\beta=-a,\\ \alpha\beta=b\end{cases}$$

と書ける．2 次方程式の解の公式とは，逆に α と β を a と b の式で表す式，ということである．α と β の置換という立場から見るとき，ここで不思議な現象が起こっていることが見て取れる．$a=-\alpha-\beta$ も $b=\alpha\beta$ も，α と β を入れ替えても不変な式なのに，最終目標の「解の公式」は，α を（あるいは β を）a と b の式として表しているわけだが，α も β も，α と β の置換に関し

て不変な式ではない．α と β を入れ替えたら，α は β になってしまうのである．何を当り前のことを，とお感じになるかも知れないが，次のような考察をすると，その不思議さが浮き立ってくる．$f(\alpha,\beta), g(\alpha,\beta)$ はともに α と β の式で，α と β を入れ替えても不変になるような式であるとする．すると，$f+g, f-g, f\times g, f\div g$ というような式はすべて α と β の入れ替えによって不変に保たれる式になってしまうのだ．証明はメチャクチャ簡単，例えば

$$\begin{aligned}(f+g)(\beta,\alpha) &= f(\beta,\alpha)+g(\beta,\alpha)\\ &= f(\alpha,\beta)+g(\alpha,\beta)\\ &= (f+g)(\alpha,\beta)\end{aligned}$$

といった具合である．ということは，a と b を使っていくら四則演算を複雑に組み合わせても，α と β の入れ替えで不変な式しか得られない．つまり，$\alpha^2+\beta^2$ とか $\alpha^3+\beta^3$ のような式なら解と係数の関係を使って a と b の多項式として表されるわけだが，α とか β とか自身を表そうとすると何か四則演算以外のものを使って**対称性**を崩さなければならないのである．ここで「対称性」という言葉を使ったが，線対称とか点対称とかの対称性とは，何かの操作をして不変だという性質であるので，置換による不変性も，まさに式の対称性を表すことになる．図形の対称性は目で見てすぐわかるわけだが，このような式の対称性や，物理法則が座標の取り方によらない，というような目で見えない対称性は重要な役割を果たすことが多い．2 次方程式の場合は，平方根を使って対称性を崩すことになる．実際，解の公式 $\frac{-a\pm\sqrt{a^2-4c}}{2}$ のルートの中身を見てみると，$a^2-4c=(\alpha+\beta)^2-4\alpha\beta=\alpha^2-2\alpha\beta+\beta^2=(\alpha-\beta)^2$ となり，これは対称式であるが，その平方根を取った式 $\alpha-\beta$ は，α と β を入れ替えると $\beta-\alpha$ に変わるので，不変ではなくなっている．

7. ラグランジュの置換（3, 4, 5 次方程式）

3 次方程式の場合，ラグランジュの考察は，さらに面白い現象を表に出してくれる．$x^3+ax^2+bx+c=0$ という 3 次方程式の 3 つの解を α,β,γ とすると，解と係数の関係により

$$\begin{cases}\alpha+\beta+\gamma=-a,\\ \alpha\beta+\beta\gamma+\gamma\alpha=b,\\ \alpha\beta\gamma=-c\end{cases}$$

となる．a,b,c を四則演算でいくら組み合わせても α,β,γ の入れ替えで不変な式しか作れないので，解の公式を作ろうと思うと平方根や 3 乗根で対称性を崩さないといけない，という事情は同じだ．

ファンデルモンドの行列式

$$\begin{vmatrix}1 & \alpha & \alpha^2\\ 1 & \beta & \beta^2\\ 1 & \gamma & \gamma^2\end{vmatrix}=(\beta-\alpha)(\gamma-\alpha)(\gamma-\beta)$$

というのは見たことがあるだろう．行列式が差積で表されるわけだ．この式は，例えば $\alpha\mapsto\beta\mapsto\gamma\mapsto\alpha$ という置換を行うと不変だが，α と β だけを入れ替えると -1 倍になる．偶置換では不変になり，奇置換だと -1 倍になるという性質を持っているので，偶置換・奇置換の定義に用いられることもある．3 つの解の置換なので，$3!=6$ 通りの入れ替え方があるわけだが，そのうちちょうど半分の 3 つで不変，残り 3 つでは他の式に変化してしまう，という中途半端な対称性を持っている式なのである．置換の考え方によって，完全に対称でない式に対しても「どれくらい対称か」という程度を表すことができるようになったわけだ．

ところで，ファンデルモンドの行列式を 2 乗すると，偶置換奇置換に関わらず不変な式になる．この差積の 2 乗を，a,b,c を使って表すことができる．具体的には

$$\begin{aligned}&\big((\beta-\alpha)(\gamma-\alpha)(\gamma-\beta)\big)^2\\ &=-27c^2-4a^3c+18abc+a^2b^2-4b^3\end{aligned}$$

となる．特に $a=0$ のときは $-27c^2-4b^3$ となるが，これはまさに定数倍を除いて，タルタリアの公式における平方根の中身だ！ 実際，$x^3+px+q=0$ の根を α,β,γ とすると，$\alpha+\beta+\gamma=0$ であり，

$q^2+\frac{4p^3}{27}$ は差積の $-\frac{1}{27}$ 倍なのである．したがってタルタリアの解法も，平方根を取ることによって，すべての置換によって不変だった a,b,c の対称性を崩して，偶置換でのみ不変になるような式を作る，という操作をやっていたわけだ．

平方根を取るとプラスマイナスの不定性があるので，置換によって ±1 倍に変化するような式を作れば良かったわけだが，3 乗根を取ると 1 倍，ω 倍，ω^2 倍という 3 通りの不定性がある．そこで，置換によって ω 倍されたり ω^2 倍されたりするような式として，$\alpha+\omega\beta+\omega^2\gamma$ という式を考えよう．この式の 3 乗は，偶置換では不変になる：

$$(\alpha+\omega\beta+\omega^2\gamma)^3+a^3+\frac{9ab}{2}-\frac{27c}{2}$$
$$=-\frac{3\sqrt{-3}}{2}(\beta-\alpha)(\gamma-\alpha)(\gamma-\beta).$$

同様に $\alpha+\omega^2\beta+\omega\gamma$ の 3 乗は，この -1 倍となる．特に α,β,γ が $x^3+px+q=0$ の解なら $\alpha+\omega\beta+\omega^2\gamma$ と $\alpha+\omega^2\beta+\omega\gamma$ は

$$\sqrt[3]{\frac{-27q}{2}\pm3\sqrt{-3}\sqrt{-27q^2-4p^3}}$$

と表され，これに $\alpha+\beta+\gamma=0$ を加えて 3 で割ったものがちょうどタルタリアの公式となるわけである．

4 次方程式についても，同様の考察を行うことができる．フェラーリの解法の中で現れた k は，4 次方程式の 4 つの解を $\alpha,\beta,\gamma,\delta$ とすると，$k=\frac{\alpha\beta+\gamma\delta}{2}$ となるのである．$\alpha\beta+\gamma\delta$ の対称性は高く，$\alpha,\beta,\gamma,\delta$ をいろいろと置換したとき，その結果として得られる式は $\alpha\beta+\gamma\delta$ の他に $\alpha\gamma+\beta\delta,\alpha\delta+\beta\gamma$ の 2 通り，計 3 つしかない．これが，k が 3 次方程式の解として得られる理由であり，それを解いて k を特定するところから対称性を崩していくわけである．

8. ガロア理論

ラグランジュの考察の目標は，5 次方程式に解の公式がない理由を説明しよう，というものだったが，それを達成したのがアーベルとガロアであった．アーベルは解の公式がないことを証明したが，ガロアはさらに進んで，どのような方程式であれば四則演算と冪根で解を書き下せるか，まで解き明かした．そのアイデアの基本線はラグランジュのものだが，ラグランジュが置換の「個数」に着目したのに対し，ガロアは置換の「構造」に目を向けたのである．n 次方程式の解の「自然な入れ替え」(今の言葉で言えば，分解体の同型を導くようなもの，つまりガロア群）は群をなし，解の有理式 f を不変にするようなもの全体は，部分群をなす．ラグランジュもそこまでは気付いていたが，ガロアが気付いたことは，素数冪の冪根（例えば 12 乗根は 2 乗根の 2 乗根の 3 乗根なので，素数冪の冪根のみを考えて一般性を失わない）を取ることによって対称性を崩す場合，それによって「それまで得られた式」をすべて不変にするような部分群は小さくなるわけだが，それが直前の不変部分群の正規部分群となり，しかも商群が巡回群になる，ということである．したがって，解の「自然な入れ替え」の群が，そのような部分群の列を持たない場合，四則演算と冪根によって解を書き下すことはできない．ガロアは，素数次の既約方程式のガロア群がそのような部分群の列を持つための必要十分条件が，解のうち任意の 2 つがわかると他の解がその 2 解の有理式で書けることである，と証明した．例えば，実係数の 5 次方程式が 3 つの実数解と 2 つの虚数解を持つ場合，実数解 2 つを取って有理式としてどう組み合わせても虚数解を表すことはできないので，その 5 次方程式の解は四則と冪根では表されないのである．

9. ガウスの正 17 角形

ガロア理論によれば，逆にガロア群が可解群であれば（つまり上記のような部分群の列があれば)，解を四則演算と冪根で書き下すことができる．ガロア以前に，その辺の筋書きをほぼ見抜いていた男がいた．ガウスである．ガウスは研究成果を発表するのに慎重で，よほど明快に説明できないと成果を秘密にしてしまう，という悪い癖があった

が，そのガウスが19才のときに発見して，喜び勇んで発表したのが，正17角形の作図可能性であった．作図と方程式は関係がなさそうだが，正17角形を作図するには，方程式 $z^{17}=1$ の解を複素平面上にプロットすれば良い．解のうち一つ $z=1$ が簡単に見つかるので，$z-1$ で割って $z^{16}+z^{15}+\cdots+z^2+z+1=0$ を解けば良い．$\varphi=\frac{2\pi}{17}$ と書くことにして，$\zeta=\cos\varphi+i\sin\varphi$ とおくと，$\zeta,\zeta^2,\cdots,\zeta^{16}$ が解の全体なので，分解体の同型は ζ の行き先を定めれば決定する．その行き先は ζ^i のうちのどれかなので，$\sigma(\zeta)=\zeta^3$ と定めると，ガロア群は $\{\sigma,\sigma^2,\cdots,\sigma^{16}=\mathrm{id}\}$ という位数16の巡回群となる．このうち，$\zeta+\zeta^{16}=\zeta+\sigma^8(\zeta)=2\cos\varphi$ を作図できれば，正17角形が作図できることになる．$\zeta+\zeta^{16}$ は（唯一の）位数2の部分群 $\{\mathrm{id},\sigma^8\}$ を固定化部分群として持つことに注意しよう．位数4の部分群 $\{\mathrm{id},\sigma^4,\sigma^8,\sigma^{12}\}$ を固定化部分群として持つ元として，

$$a:=\cos\varphi+\cos4\varphi,$$
$$b:=\cos2\varphi+\cos8\varphi,$$
$$c:=\cos3\varphi+\cos5\varphi,$$
$$d:=\cos6\varphi+\cos7\varphi$$

を取り出すことができ，さらに位数8の部分群 $\{\mathrm{id},\sigma^2,\sigma^4,\cdots,\sigma^{14}\}$ を固定化部分群として持つ元として，$e:=a+b$ と $f:=c+d$ を取る．$e+f=\sum_{i=1}^{16}\frac{\zeta^i}{2}=-\frac{1}{2}$ であり，さらに $2\cos A\cos B=\cos(A+B)+\cos(A-B)$ を使って

$$\begin{aligned}2ab&=e+f=-\frac{1}{2},\\2ac&=2a+b+d,\\2ad&=b+c+2d,\\2bc&=a+2c+d,\\2bd&=a+2b+c,\\2cd&=e+f=-\frac{1}{2}\end{aligned}$$

がわかるので，

$$ef=ac+ad+bc+bd=2(a+b+c+d)=-1$$

となる．つまり e と f は $x^2+\frac{x}{2}-1=0$ の解であって，$e>f$ より $e=\frac{-1+\sqrt{17}}{4}, f=\frac{-1-\sqrt{17}}{4}$ だとわかる．$a+b=e, ab=-\frac{1}{4}$ だったので，a と b は $4x^2+(1-\sqrt{17})x-1=0$ の解であり，

$$a,b=\frac{-1+\sqrt{17}\pm\sqrt{34-2\sqrt{17}}}{8}$$

と求まる（但し，$a>b$）．同様に

$$c=\frac{-1-\sqrt{17}+\sqrt{34+2\sqrt{17}}}{8}$$

が求まる．$\cos\varphi\cos4\varphi=\frac{c}{2}$ なので $\cos\varphi$ は2次方程式 $x^2-ax+\frac{c}{2}$ の大きいほうの解であり，$a^2=1+\frac{b}{2}$ を用いて

$$\begin{aligned}\cos\varphi&=\frac{a+\sqrt{a^2-2c}}{2}\\&=\frac{a+\sqrt{1+b/2-2c}}{2}\\&=\frac{-1+\sqrt{17}+\sqrt{34-2\sqrt{17}}}{16}\\&\quad+\frac{\sqrt{17+3\sqrt{17}-\sqrt{34-2\sqrt{17}}-2\sqrt{34+2\sqrt{17}}}}{8}\end{aligned}$$

となり，$\cos\frac{2\pi}{17}$ が四則演算とルートで表されることがわかる．四則演算とルートはコンパスと定規で作図できるので，正17角形が作図できるのである．ガウスは，「一般に p が素数のとき，$p-1$ が2の冪，例えば $p=3,5,17,257,65537$ ならば2次方程式のみが出てくる」と言っている．単に計算をした，というわけではなく，解の対称性を見通しているのである．

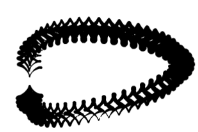
参考文献

1) 木村俊一：『天才数学者はこう解いた、こう生きた』，講談社選書メチエ（2001）．
2) 木村俊一：『ガロア理論』（数学のかんどころ14），共立出版（2012）．
3) 高木貞治：『近世数学史談』，岩波文庫（1995）．
4) J-P. Tignol（新妻弘訳）：『代数方程式のガロアの理論』，共立出版（2005）．

（きむら・しゅんいち，広島大学大学院理学研究科）

代数幾何学の面白さ

円の有理パラメーター表示からの出発



小木曽　啓示

1. 序

高校の数学に，x, y の連立方程式 $x^2+y^2=1$, $2x+y=k$ はいつ実数解をもつかという問題がある．代数の問題であるが，円 $x^2+y^2=1$ と直線 $2x+y=k$ はいつ交点をもつかという問題に翻訳することで幾何学的にも解けることに面白さを感じた読者も多いのではないかと思う．このように，式（代数）と図形（幾何）を行き来しながら考えるのが代数幾何学の一つの醍醐味である．また，円 $x^2+y^2=1$ の問題は，三角関数を用いたパラメーター表示

$$x=\cos\theta,\quad y=\sin\theta \tag{P1}$$

を考えることで，より鮮やかに解ける経験をした読者も多いと思う．大学に入り，円 $x^2+y^2=1$ の有理関数によるパラメーター表示

$$x=\frac{1-t^2}{1+t^2},\quad y=\frac{2t}{1+t^2} \tag{P2}$$

（直線 $y=t(x+1)$ の傾き t に円 $x^2+y^2=1$ との交点を対応させてできるパラメーター表示）を考えることで，$\cos\theta, \sin\theta$ の混じった複雑な積分が求められることに興味を感じた読者もいるであろう．

代数幾何学では，複素数体 $\mathbb{C}$ 上で考えることが多い．$\mathbb{C}$ は幾何学が使える代数閉体であるからである．同じ（標数が 0 の）代数閉体であっても，$\mathbb{Q}$ の代数閉包である $\overline{\mathbb{Q}}$ はより整数論的色彩が強くなる．

以下，本稿では，幾何学的イメージがより鮮明な $\mathbb{C}$ に特化して考えることにする．つまり，円は複素円

$$(x^2+y^2-1=0) := \{(a,b)\in\mathbb{C}^2 | a^2+b^2-1=0\}\subset\mathbb{C}^2$$

と考えることにする．円とはいっても複素 1 次元という意味では曲線だが，実次元では 2 次元（実曲面）である．複素円のように，$\mathbb{C}^n$ 内で多項式の共通零点集合の形に書ける集合を**アファイン代数的集合**という．複素円のパラメーター表示 (P1) は本質的に超越的となり，どの程度役立つものなのか筆者には分からないが，円の有理パラメーター表示 (P2) は複素円においてもそのまま有効であり，$\mathbb{P}^1$ の幾何学が展開できる．

本稿では代数幾何学の考え方の一端を複素円から始めて具体例を通して紹介したい．

2. 複素円のパラメーター表示と有理写像

複素円のパラメーター表示 (P2) は，ほとんどいたるところ像の定まった，有理式による写像

$$\varphi : \mathbb{C} \dashrightarrow (x^2+y^2-1=0)\subset\mathbb{C}^2,$$
$$t\mapsto\left(\frac{1-t^2}{1+t^2},\frac{2t}{t^2+1}\right)$$

を考えていることになる．φ の像が定まらない点は，極である 2 点 $t=\pm\sqrt{-1}$ である．

代数幾何学においては，アファイン集合そのものに興味がある場合でもいったんは射影空間 $\mathbb{P}^d$ にコンパクト化した後考えることが多い．

$\mathbf{0}=(0,0,\cdots,0)$ 以外の $d+1$ 個の複素数の比全体

$$\mathbb{P}^d := \{[\boldsymbol{x}]=[x_0:x_1:\cdots:x_d] | \boldsymbol{x}\in\mathbb{C}^{d+1}\setminus\{\mathbf{0}\}\}$$

が d 次元**射影空間**である．例えば $\mathbb{P}^2$ には $[0:0:0]$ という点はなく，$\mathbb{P}^2$ において $[y_0:y_1:y_2]=[x_0:x_1:x_2]$ であることと，複素数 c により，$(y_0,y_2,y_3)=c(x_0,x_1,x_2)$ と書けることは同値である．互いに逆の全単射対応

$$\mathbb{C}^2\ni(x,y)\mapsto[1:x:y]\in(x_0\neq0)\subset\mathbb{P}^2,$$

$$\mathbb{P}^2\supset(x_0\neq0)\ni[x_0:x_1:x_2]\mapsto\left(\frac{x_1}{x_0},\frac{x_2}{x_0}\right)\in\mathbb{C}^2$$

により，$\mathbb{C}^2=(x_0\neq0)\subset\mathbb{P}^2$ と見なす．このとき，

$\mathbb{P}^2$ は $\mathbb{C}^2$ に無限遠直線 $(x_0=0)$ が付け加わってコンパクト化された空間である．$(x_1\neq 0)$, $(x_2\neq 0)$ に関しても同じ考察をすれば，$\mathbb{P}^2$ は 3 枚の $\mathbb{C}^2$ が貼り合わされてできた空間でもある．$\mathbb{P}^2$ は比の集合だから，方程式 $F_d(x_0,x_1,x_2)=0$ が意味をもつのは $F_d(x_0,x_1,x_2)$ が斉次多項式の場合である．また，有理式 $f=G_d(x_0,x_1,x_2)/H_d(x_0,x_1,x_2)$ は，G_d, H_d が同じ次数の斉次多項式であるとき，$\mathbb{P}^2$ 上の関数としての意味を持ち，**有理関数**と呼ばれる．式の**斉次化**，**非斉次化**により，有理関数はアファイン座標

$$x=\frac{x_1}{x_0},\quad y=\frac{x_2}{x_0}$$

の有理式であり，逆も成り立つ．例えば，

$$\frac{(x_0^2-x_1^2)x_1}{x_0x_1x_2}=\frac{x_0^2-x_1^2}{x_0x_2}=\frac{1-x^2}{y},$$
$$\frac{1-x^2}{y}=\frac{1-(x_1/x_0)^2}{(x_1/x_0)}=\frac{x_0^2-x_1^2}{x_0x_2}$$

である．$\mathbb{P}^d$ においても同様である．

$\mathbb{P}^2$ の斉次座標 $[x_0:x_1:x_2]$ を用いれば，複素円 $(x^2+y^2-1=0)\subset\mathbb{C}^2$ は $(x_1/x_0)^2+(x_2/x_0)^2-1=0$ と書け，分母を払うことにより，$\mathbb{P}^2$ 内の曲線

$$C:=(x_1^2+x_2^2-x_0^2=0)\subset\mathbb{P}^2$$

にコンパクト化される．C は無限遠直線 $(x_0=0)$ 上の 2 点 $[0:1:\sqrt{-1}]$, $[0:1:-\sqrt{-1}]$ が複素円に付け加わった曲線である．このように射影空間内のいくつかの斉次多項式の共通零点集合を**射影代数集合**という．真の代数部分集合の有限和でかけない射影代数集合 V を**射影多様体**という．V の有理関数は $\mathbb{P}^d$ の有理関数の V への制限として定める．もちろん，V がすっぽり極に含まれるものは除外する．

同様に，ソースである $\mathbb{C}$ も $t=y_1/y_0$ により $\mathbb{P}^1$ によりコンパクト化しよう．

$$\left[1:\frac{1-t^2}{1+t^2}:\frac{2t}{1+t^2}\right]=[1+t^2:1-t^2:2t],$$
$$=\left[1+\left(\frac{y_1}{y_0}\right)^2:1-\left(\frac{y_1}{y_0}\right)^2:2\frac{y_1}{y_0}\right]$$
$$=[y_0^2+y_1^2:y_0^2-y_1^2:2y_0y_1]$$

だから，写像 φ は

$$\varphi:\mathbb{P}^1\to C,\quad [y_0:y_1]\mapsto[y_0^2+y_1^2:y_0^2-y_1^2:2y_0y_1]$$

といういたるところ正則な写像に延長される（像が $[0:0:0]$ になってしまうような $\mathbb{P}^1$ の点 $[y_0:y_1]$ はないことにも注意しよう）．また，φ の逆写像 ψ が，対応

$$[x_0:x_1:x_2]\mapsto[x_0+x_1:x_2]=[x_2:x_0-x_1]$$

で与えられる．最後の等式では C において $(x_0-x_1)(x_0+x_1)=x_2^2$ であることを用いている．ψ の像の第 1 表示では C の点 $[1:-1:0]$ の像は $[0:0]$ となり定まらないように見えるが，像の第 2 表示により $[0:2]=[0:1]$ と確かに定まっていることが重要である．非斉次化すれば，φ,ψ は，ともに有理関数で表される正則な写像である．こうして $\mathbb{P}^1$ は $\mathbb{P}^2$ の 2 次曲線 C と同型（双正則）になる．

このように有理関数の組で与えられる写像を**有理写像**という．すべての点で像の定まる有理写像が**正則写像**である．ある稠密な部分集合上一致する有理写像は同じ有理写像と考える．有理関数は大域的かつ剛 (rigid) であるため，稠密集合上での値の一致により決まってしまうからである．例えば，有理写像 $t\mapsto 1/t$ を 2 回合成したものは有理写像として id である．有理写像を用いて射影多様体を調べることは代数幾何学の基本である．有理関数の形が具体的に書けないときでも，射影多様体間の有理写像は，因子の線形系というより幾何学的な道具を用いて記述できる．その利点は層係数 cohomology 理論や交点理論との相性がとてもよい点にある．

3. 楕円曲線と有理微分形式

本節では，「複素曲線

$$C_\lambda=(y^2-x(x+1)(x-\lambda)=0)\subset\mathbb{C}^2$$

（$\lambda\in\mathbb{C}$ は定数）は有理関数を用いてパラメーター付け $x=f(t), y=g(t)$ できるか？」という問題を考える．複素円は 2 次曲線だったが，C_λ は 3 次曲線である．

まず，$\lambda=0$ の場合を見てみよう．

$$C_0=(y^2=x^2(x+1))\subset\mathbb{C}^2$$

である．複素円と異なり，C_0 は特異点 $(0,0)$ をもつ．C_0 の原点以外の点はすべて滑らかである．

$$f=\frac{\partial f}{\partial x}=\frac{\partial f}{\partial y}=0\quad (f:=y^2-x^2(x+1))$$

の複素解は $(x,y)=(0,0)$ のみだからである（Jacobian 判定法）．C_0 のパラメーター付けの問題に戻ろう．直線 $y=tx$ は原点で C_0 と “2 重以上に” 交わるはずである．原点は特異点だからである．従って，$y=tx$ と C_0 の交点 $(x(t),y(t))\neq(0,0)$ が，ほとんどの t に対し一つに決まるはずである．C_0 は 3 次式だからである．この対応で C_0 はパラメーター付けできるのでは？と推測できる．実際に計算を遂行すると，

$$(x(t)=t^2-1, y(t)=t(t^2-1))$$

とわかる．推測通りパラメーター付けできたのである．このパラメーター付けを，前節同様，有理写像

$$\nu : \mathbb{C} \to C_0, \quad t \mapsto (t^2-1, t(t^2-1))$$

と見てみよう．ν の形から，特異点 $(0,0)$ の逆像は 2 点 ± 1 である．また，他の点の逆像はすべて 1 点である．より強く，

$$\nu | \mathbb{C} \setminus \{\pm 1\} : \mathbb{C} \setminus \{\pm 1\} \to C_0 \setminus \{(0,0)\}$$

は同型写像である．逆写像が正則な有理関数 $t = y/x$ で与えられるからである．このことからも C_0 は原点を除き滑らかであることがわかる．$\mathbb{C}$ は滑らかだからである．従って，C_0 からみれば，パラメーター付け $\nu : \mathbb{C} \to C_0$ は C_0 の特異点解消写像である．このように式を図形と関係付けることで，式のもつより深い意味を探ることも代数幾何の醍醐味の一つである．後に，blow up と呼ばれる写像と関係付けることでより鮮明な幾何学的意味を与える．同様の方法で，$\lambda = -1$ の場合も特異点解消を与えるパラメーター付けができる（各自試みられたい）．

一般に，2 つの多様体 V, W の間に $g \circ f = \mathrm{id}_V$, $f \circ g = \mathrm{id}_W$ をみたす有理写像 $f : V \dashrightarrow W$ と $g : W \dashrightarrow V$ があるとき，V と W は**双有理**であるという．例えば，$\mathbb{C}$ と C_0 は双有理である．$\mathbb{P}^1$ と双有理である射影曲線のことを**有理曲線**という．C_0 の $\mathbb{P}^2$ でのコンパクト化は有理曲線である．$\mathbb{C}$ のコンパクト化 $\mathbb{P}^1$ と双有理だからである．代数多様体 V の点 P は，P において次元個の有理関数からなる局所座標がとれるとき，**非特異**（**滑らかな**）点であるという．例えば，C_0 の点 $\mathrm{P} \neq (0,0)$ は滑らかな点である．Jacobian 判定法により，$x - x(\mathrm{P})$ または $y - y(\mathrm{P})$ が P における局所座標にとれるからである．ここで V の次元は V の複素次元であり，代数的には V の有理関数体 $\mathbb{C}(V)$（V の有理関数全体のなす体）の $\mathbb{C}$ 上の超越次数である．直感的には超越基底は V 上自由に動ける最大個数のパラメーターだからである．C_0 の有理関数体 $\mathbb{C}(C_0) = \mathbb{C}(x,y)$ では $y^2 = x^2(x+1)$ である．従って y は $\mathbb{C}(x)$ 上代数的であり，$\mathbb{C}(C_0)$ の超越次数は確かに 1 である．

以下，$\lambda \neq 0, -1$ の場合を考える．C_λ を $\mathbb{P}^2$ の曲線にコンパクト化すると，$(x_0 = 0)$ 上の点 $\infty = [0:0:1]$ が付け加わった曲線

$$E_\lambda = (x_2^2 x_0 - x_1(x_1+x_0)(x_1 - \lambda x_0) = 0) \subset \mathbb{P}^2$$

となる．Jacobian 判定法により，E_λ は滑らかな曲線である（$[0:0:1]$ も忘れず調べることが大切である）．ある $E_\lambda (\lambda \neq 0, -1)$ と同型な曲線を**楕円曲線**という．楕円曲線は有理曲線とともに，頻繁にでてくる重要な曲線である．

パラメーター付けの問題は，有理写像 $\varphi : \mathbb{P}^1 \dashrightarrow E_\lambda$ の存在・非存在を問う問題である．φ は存在すれば正則写像になる．なぜならば，$\mathbb{P}^1$ の各点 P における局所座標 t_{P} を考えれば

$$[1 : f(t) : g(t)] = [t_{\mathrm{P}}^n : t_{\mathrm{P}}^n f(t) : t_{\mathrm{P}}^n f(t)]$$

であり，P において，整数 n で調整することによって，右辺の各項は正則かつ $[0:0:0]$ でないようにできるからである．このように滑らかな曲線から射影空間への写像は常に正則である．従って，滑らかな射影曲線の双有理幾何は双正則幾何と同じである．

元に戻って，E_λ の有理 1 形式 $\omega = dx/y$ を考えてみよう．ω は見かけ上 $y = 0$ において極を持つようにみえるが実はどこにも極を有しない．すなわち，正則 1 形式である．なぜならば，$f = y^2 - x(x+1)(x-\lambda)$ とおくとき，$y = 0$ である点 P においては，$\partial f / \partial x \neq 0$ だから，$y_{\mathrm{P}} = y - y(\mathrm{P})$ が局所座標を与えるからである．

$$0 = df = 2ydy - ((x+1)(x-\lambda) + x(x-\lambda) + (x+1)x)dx$$

だから，P においては

$$\omega = \frac{2dy}{(x+1)(x-\lambda) + x(x-\lambda) + (x+1)x}$$

であり分母は P において 0 でないからである．点 ∞ でも同様に正則である．

従って，もしパラメーター付け φ があれば，φ の正則性により，$\varphi^* \omega$ は $\mathbb{P}^1$ の（恒等的には 0 でない）正則な有理 1 形式のはずである．

ところが $\mathbb{P}^1$ には正則な有理 1 形式は 0 以外にはない．$\mathbb{P}^1$ の有理 1 形式 $\eta \neq 0$ は $\mathbb{C}$ で正則であるなら，$h(t)dt$（$h(t)$ は t の 0 以外の多項式）の形であるが，$t = \infty$ における局所座標は $s = 1/t$ であり，∞ の近くでは

$$\eta = f(t)dt = -f\left(\frac{1}{s}\right)\frac{ds}{s^2}$$

である．このとき，$t = \infty$ において $\deg f(t) + 2$ 位の極をもつからである．従って，パラメーター付けできない．

このように有理写像と有理形式を用いた幾何が代数幾何学の主要な手法である．d 次元においては有理 d 形式が最重要になる．有理形式は一見超越的にみえるが，必要な微分は有理式の微分だけであるため，実は純代数的である．

4. 爆発（blow up）

次元をあげて 2 次元の場合を観察してみよう．本質的な意味で像の定まらない有理写像が現れる．その解消が blow up である．

射影平面 $\mathbb{P}^2$ を考え，$[x_0 : x_1 : x_2]$ をその斉次座標とする．$x = x_1/x_2$, $y = x_2/x_0$, $y/x = x_2/x_1$ は $\mathbb{P}^2$ の有理関数である．有理関数 y/x の定める有理写像

$$\pi : \mathbb{P}^2 \dashrightarrow \mathbb{P}^1, \quad [x_0 : x_1 : x_2] \mapsto [x_1 : x_2]$$

を考えてみよう．$\mathbb{P}^1$ には点 $[0 : 0]$ がないため，$\mathrm{O} := [1 : 0 : 0]$ における像が定まっていない．実は O では本質的な意味で像が定まらない．O と $[0 : a : b]$ を結ぶ直線 $L_{[a:b]} = (bx_1 - ax_2 = 0)$ 上の点 $\mathrm{P} \neq \mathrm{O}$ の像は $L_{a,b}$ の方向である $[a : b]$ であり $L_{[a:b]}$ 上 O を除き一定である．もし，π が 0 に正則に延長できたなら，$\lim_{\mathrm{P}\to\mathrm{O}} \pi(\mathrm{P}) = \pi(\mathrm{O})$ であるが，P を直線 $L_{[a:b]}$ にそって O に近づけたときの極限は $[a : b]$ であり，近づけ方によって極限が変わってしまうからである．このように正則に延長できない点を**不確定点**という．

不確定点をなくすために，$\pi|\mathbb{P}^2 \setminus \{\mathrm{O}\}$ のグラフ

$$\Gamma^0 = \{(\mathrm{P}, \pi(\mathrm{P}))|\mathrm{P} \in \mathbb{P}^2 \setminus \{\mathrm{O}\}\} \subset \mathbb{P}^2 \times \mathbb{P}^1$$

を考えその閉包を Γ としよう．$\mathbb{P}^1$ の斉次座標を $[y_1 : y_2]$ とする．Γ^0 は $[x_1 : x_2] = [y_1 : y_2]$, $[x_1 : x_2] \neq [0 : 0]$ で定まる部分集合である．従って

$$\Gamma = (x_1y_2 - x_2y_1 = 0) \subset \mathbb{P}^2 \times \mathbb{P}^1$$

である．Jacobian 判定法より，Γ は滑らかである．

第 1 射影 $p_1 : \Gamma \to \mathbb{P}^2$ を見てみよう．$\mathbb{P}^2 \setminus \{\mathrm{O}\}$ 上は逆正則写像 $[x_0 : x_1 : x_2] \mapsto ([x_0 : x_1, x_2] : [x_1 : x_2])$ をもち，p_1 は同型である．O のファイバーは

$$E_{\mathrm{O}} := p_1^{-1}(\mathrm{O}) = \{[1 : 0 : 0]\} \times \mathbb{P}^1 \simeq \mathbb{P}^1$$

である．従って，p_1 は $E_0 \simeq \mathbb{P}^1$ を O に収縮する双有理全射正則写像，逆にみた p_1^{-1} は一点 O だけを E_{O} に爆発させる双有理写像である．$p_1 : \Gamma \to \mathbb{P}^2$，あるいは p_1^{-1} のことを $\mathbb{P}^2$ の O における**爆発（blow up）**という．また，曲線 E_{O} のことを**例外曲線**という．有理写像として，$\pi = p_2 \circ p_1^{-1}$ である．爆発 p_1^{-1} により，π を $p_2 : \Gamma \to \mathbb{P}^1$ におきかえることで不確定点を解消したことになる．

$\mathrm{P} \in L_{[a:b]}$ に対し，$\lim_{\mathrm{P}\to\mathrm{O}} p_1^{-1}(\mathrm{P}) = ([1 : 0 : 0], [a : b])$ だから，E_{O} は O における正則接ベクトル空間 $T_{\mathbb{P}^2,0}$ を射影化した $\mathbb{P}^1$ であり，blow up は O の近くで決まる局所的改変操作である．このことに着目すれば，今の構成は，任意の滑らかな曲面 $S(\subset \mathbb{P}^N)$ に対する blow up に自然に拡張できる．

S の点 P における局所座標 (x, y) を P での $\mathbb{P}^N$ のアファイン座標の一部として与えられる局所座標にとる（定義からも Jacobian 判定法からも可能である）．U_{P} を P の近傍とし，有理写像

$$U_{\mathrm{P}} \dashrightarrow \mathbb{P}^1, \quad (x(\mathrm{Q}), y(\mathrm{Q})) \mapsto [x(\mathrm{Q}) : y(\mathrm{Q})]$$

（$\mathrm{Q} \in U_{\mathrm{P}}$）の $U_{\mathrm{P}} \setminus \{\mathrm{P}\}$ 上のグラフの $U_{\mathrm{P}} \times \mathbb{P}^1$ における閉包を Γ_{P} とする．$\mathbb{P}^2$ のときと同じ理由で

$$\Gamma_{\mathrm{P}} = (xy_2 - yy_1 = 0) \subset U_{\mathrm{P}} \times \mathbb{P}^1,$$

Γ_{P} は滑らか，第 1 射影 $p_1 : \Gamma_{\mathrm{P}} \to U_{\mathrm{P}}$ は P の外では同型，そして

$$E_{\mathrm{P}} := p_1^{-1}(\mathrm{P}) = \{\mathrm{P}\} \times \mathbb{P}^1 \simeq \mathbb{P}^1$$

であり，E_{P} は P の接ベクトル空間の射影化であることがわかる．p_1 の導く同型 $\Gamma_{\mathrm{P}} \setminus E_{\mathrm{P}} \simeq U_{\mathrm{P}} \setminus \{\mathrm{P}\}$ により，$S \setminus \{\mathrm{P}\}$ と U_{P} を貼り合わせてできる曲面を $\tilde{S}$ とし，P における S の blow up を

$$p = (\mathrm{id}_{S\setminus\{P\}}, p_1) : \tilde{S} \to S$$

と定めるのである．$\tilde{S}$ は滑らかであり，$E_{\mathrm{P}} := p^{-1}(\mathrm{P}) \simeq \mathbb{P}^1$ である．また，

$$\Gamma_{\mathrm{P}} = U_1 \cup U_2, \quad U_1 := (y_1 \neq 0), \quad U_2 := (y_2 \neq 0)$$

であり，U_1 では $(x, t = y_2/y_1)$ が，U_2 では $(y, s = y_1/y_2)$ が，それぞれ座標系に選べる．E_P は，U_1 においては $(x = 0)$ で表される曲線であり，U_2 においては $(y = 0)$ で表される曲線である．また，U_1 においては $y = xt$, U_2 においては $x = ys$ である．この構成の利点は局所座標系が明示的であるため，局所的な解析がしやすい点にある．

$\mathbb{C}^2$ の原点での blow up $p : \tilde{\mathbb{C}^2} \to \mathbb{C}^2$ を考え，前節の曲線 $C_0 : (y^2 = x^2(x + 1))$ が p によりどう変わるか調べよう．U_1 上 $y = tx$ なので，全逆像 p^*C_0 は，U_1 上は $(tx)^2 = x^2(x+1)$ で表される曲線である．すなわち，2 曲線 $x^2 = 0$ と $t^2 = x + 1$ になり，例外曲線 E_{O}（2 重）と $C_0 \setminus \{0\}$ の逆像の閉包 C' の和である．C' は $t^2 = x + 1$ で与えられるから滑らかである（U_2 での検証も必要である）．従って，$p|C' : C' \to C_0$ は爆発による特異点解消になっている．$C' \cap E_0$ は 2 点 $(x, t) = (0, \pm 1)$ であり，C は原点で $y = \pm x$ のようになっていることと整合的である．前節での見方よりもより幾何学的で面白いのではないかと思う．

S の blow up は次のように大域的にも構成できる．$\mathrm{P} \in S \subset \mathbb{P}^N$ を $\mathrm{P} = [1 : 0 : \cdots : 0] =: \mathrm{O}$ となるよう

射影線形群 $\mathrm{PGL}(N+1,\mathbb{C})$ を用いて直しておく．このとき

$$\mathbb{P}^N \dashrightarrow \mathbb{P}^{N-1}, \quad [x_0 : x_1 : \cdots : x_N] \mapsto [x_1 : \cdots : x_N]$$

のグラフの閉包 Γ は $\mathbb{P}^N$ の点 O を $T_{\mathbb{P}^N,\mathrm{O}}$ の射影化である $\mathbb{P}^{N-1}$ におきかえた多様体であることが $\mathbb{P}^2$ の場合と同様にわかる．第 1 射影 $p_1 : \Gamma \to \mathbb{P}^N$ による $S \backslash \{\mathrm{P}\}$ の逆像をとり，その閉包を $\tilde{S}$ とする．このとき，制限写像 $p_1|\tilde{S} : \tilde{S} \to S$ は S の P での blow up である．P の近傍での S の局所座標を $\mathbb{P}^N$ の P におけるアファイン座標の一部であるように選んでおいたからである．特に $\tilde{S}$ も射影多様体になる．$([x_i],[y_j]) \mapsto [x_i y_j]$ で与えられる埋め込み $\mathbb{P}^n \times \mathbb{P}^m \to \mathbb{P}^{(n+1)(m+1)-1}$ により，$\mathbb{P}^n \times \mathbb{P}^m$ は自然に射影多様体となるからである．$\tilde{S}$ と S は双有理であり，集合論的，代数的には非常に似たものであるが，幾何学的には同相ですらない．例外曲線 E_{P} により，$b_2(\tilde{S}) = b_2(S)+1$ だからである．

5. 曲面の交点理論と標準因子

本節では 2 次元（1 次元）射影多様体のことを単に曲面（曲線）という．S を滑らかな曲面とする．

S の既約な曲線（2 つ以上の曲線の和に分解できない S の曲線）全体を $\mathbb{Z}$-自由基底とするアーベル群を $\mathrm{Div}\,(S)$ と書く．$2-1=1$ なのでやや紛らわしいが以下しばらくは，曲面上の曲線は余次元 1 であることが重要である．$\mathrm{Div}\,(S)$ の元を S の**因子**という．すべての係数が非負である因子を**有効因子**という．例えば，$\mathbb{P}^2$ の 2 直線 $L_1 = (x_1 = 0)$, $L_2 = (x_2 = 0)$ は既約な曲線であり，$2L_1 + L_2$ は有効因子，$L_2 - L_1$ は有効でない因子である．0 でない有理関数 f に対し，因子 (f) を

$$(f) = \sum_{i=1}^{k} m_i C_i, \quad m_i := \mathrm{ord}_{C_i}(f)$$

と定め，f の定める**主因子**という．係数 m_i は $m_i > 0$ のときは f は C_i にそってちょうど m_i 重の零をもつことを意味し，$m_j < 0$ のときは f は C_j にそってちょうど $-m_j$ 重の極をもつことを意味する．係数 m_i は対応する曲線の十分一般の点において調べればよい．S の曲線はその稠密部分集合から，閉包をとることで復元できるからである．例えば，$\mathbb{P}^2$ の有理関数 x_1/x_2 に対し $\mathrm{div}(x_1/x_2) = L_1 - L_2$ である．$D' - D$ が主因子であるとき，2 つの因子 D と D' は**線形同値**といい，$D' \sim D$ とかく．商集合 $\mathrm{Div}(S)/\sim$ のことを $\mathrm{Pic}\,(S)$ と書き，S の**ピカール群**という．$\mathrm{Pic}\,(S)$ は自然にアーベル群である．

例えば，$\mathbb{P}^2$ の有効因子はすべて $(F_d = 0)$（F_d は 0 以外の d 次斉次多項式）の形である．$\mathbb{C}[x_0, x_1, x_2]$ は UFD（一意分解整域）だからである．F_d/x_0^d は大域的有理関数だから，$\mathbb{P}^2$ の因子は dH（$H = (x_0 = 0), d \in \mathbb{Z}$）のどれかに線形同値である．特に，$\mathrm{Pic}\,(\mathbb{P}^2) = \mathbb{Z}H$（$H$ で H の類を表している）である．

S は滑らかとしているので，S の因子は S の各点の近傍で局所的には有理関数の主因子の形になる．すなわち，S の（アファイン）開被覆 $S = \cup U_i$ を十分小さくとれば D は U_i 上は一つの有理関数 h_i の主因子となる．そのため，$g_{ij} = h_i/h_j$ は $U_i \cap U_j$ 上すべての点で正則かつ非零となり，$\{g_{ij}\}$ を変換関数系とする S 上の直線束 $[D]$ ができる．D は大域有理切断 $\{h_i\}$ に対応する因子，すなわち，その零と極の因子として復元される．D の 0 でない大域有理切断全体は $\mathbb{C}^\times$ 倍を法として，D の線形同値な因子と $1:1$ 対応の関係にある．対応は大域有理切断の零・極の定める因子を対応させる自然なものである．S の大域的正則関数は定数のみだからである．特に，$D' \sim D$ であることと直線束として $[D'] \simeq [D]$ であることは同値である．また，$[D]$ の 0 でない大域的正則切断全体は $\mathbb{C}^\times$ 倍を法として D と線形同値な有効因子と $1:1$ 対応の関係にある．

以上を踏まえて，S の因子 D（余次元 1）と既約曲線 C（次元 1）の**交点数**を

$$(D.C) := \deg \nu^*[D]$$

と定める．ここで $\nu : \tilde{C} \to C$ は曲線 C の特異点解消（＝正規化）であり，$\deg \nu^*[D]$ は 0 でない大域的有理切断の重複度をこめた零点の個数から極の個数を引いた数である．正規化の存在と一意性，直線束は自然に引き戻せること，代数的な構成なので必ず有理切断があることおよび曲線の主因子は次数 0 であること（留数定理）から well-defined である．ここでは C の次元が 1 であることが重要である．因子 D と一般の因子 $C = \sum_{i=1}^{k} m_i C_i$ の交点数は $\sum_{i=1}^{k} m_i (D.C_i)$ と定める．定義から，$D \sim D'$ ならば $(D.C) = (D'.C)$ である，また，$(D.C)$ は D についても C についても線形である．

既約曲線 C と因子 D に対し，$C \cap \mathrm{Supp}\,D = \emptyset$ ならば，$(D.C) = 0$ である．D に対応する $[D]$ の有理切断は C に零も極ももたないからである．また，曲線 C, D が滑らかな部分のみで横断的に交わっていれば $(D.C)$ は集合 $C \cap D$ の元の個数，すなわち，素朴な意味での交点数である．D の局所方程式系 $\{f_i\}$ の定

める $[D]$ の大域的正則切断の C への制限がそのまま $\nu^*[D]$ の正則切断になるからである．このことと，超平面切断類は豊富であることを使って，横断的に交わる状況に帰着させることで $(D.C)$ は D と C について対称であることもわかる．このように交点数の定義は直感に十分に合ったものである．注意も要する．例えば，先に出てきた $\mathbb{P}^2$ の因子 L_1 に対し，L_1 と L_1 の交点数は（∞ ではなく）

$$(L_1.L_1) = (L_2.L_1) = 1$$

である．L_1 と L_2 は線形同値で，L_1 と L_2 は 1 点で横断的に交わるからである．従って，先の H に対し，$(H.H) = 1$ であり，$H \not\sim 0$ である．特に，$\mathrm{Pic}\,(\mathbb{P}^2) = \mathbb{Z}H \simeq \mathbb{Z}$ である．

S の零でない有理 2 形式 ω の零と極から定まる因子を**標準因子**という．曲線の場合と同様に曲面の場合にも非常に重要な因子である．また，ω' が別の有理 2 形式であれば，$\omega' = f\omega$ $(f \in \mathbb{C}(V))$ とかけ，標準因子はすべて線形同値である．正確には有理 2 形式の因子の線形同値類が標準因子 K_S である．K_S を求めるには，$\mathbb{C}(S)$ の超越基底 f_1, f_2 に対し $df_1 \wedge df_2$ の因子を求めればよい．それには，S の各点 P における局所座標 $(x_{\mathrm{P}}, y_{\mathrm{P}})$ を用いて，$df_1 \wedge df_2$ を $f_{\mathrm{P}}dx_{\mathrm{P}} \wedge dy_{\mathrm{P}}$ の形にすることで，f_{P} の零と極をみればよいことになる．例えば，$K_{\mathbb{P}^2} = -3H$（線形同値の意味で）である．$dx \wedge dy$ $(x = x_1/x_0,\ y = x_2/x_0)$ の因子を調べればよいが，問題となるのは $(x_0 = 0)$ 上だから新しい座標 $w = x_0/x_1, u = x_2/x_1$ の式に直すことで確認できる．特に，次が従う：

$$(K_{\mathbb{P}^2}.K_{\mathbb{P}^2}) = (-3H.-3H) = 9.$$

$\mathbb{C}^2 = \mathbb{C} \times \mathbb{C}$（座標は x, y）と考えると，$\mathbb{C}^2$ の別のコンパクト化 $\mathbb{P}^1 \times \mathbb{P}^1$ ができる．特に，$\mathbb{P}^2$ と $\mathbb{P}^1 \times \mathbb{P}^1$ は双有理である．他方，$\mathbb{P}^1 \times \mathbb{P}^1$ の有理 2 形式 $dx \wedge dy$ の因子は $-2(h_1 + h_2)$ $(h_1 = \{\infty\} \times \mathbb{P}^1,\ h_2 = \mathbb{P}^1 \times \{\infty\})$ である（先と同じ方法でわかる）．h_1 は第 1 射影の任意のファイバーと線形同値だから，$(h_1.h_1) = 0$ である．同様に $(h_2.h_2) = 0$ である．また h_1, h_2 は一点で横断的に交わるから $(h_1.h_2) = 1, (h_2.h_1) = 1$ である．以上から，次が従う：

$$(K_{\mathbb{P}^1 \times \mathbb{P}^1}.K_{\mathbb{P}^1 \times \mathbb{P}^1}) = (-2(h_1 + h_2).-2(h_1 + h_2)) = 8.$$

このことからも，$\mathbb{P}^2$ と $\mathbb{P}^1 \times \mathbb{P}^1$ は**双有理だが同型ではない**ことがわかる．もし，同型であったなら，同型を与える写像で標準因子類と交点数は保たれるはずだからである．このように交点理論を用いて数値的情報から幾何学的結論を導くことも代数幾何学の主要な方法の一つである．

6. 例外曲線の自己交点数と収縮定理

S を滑らかな射影曲面，$p : \tilde{S} \to S$ を S の点 P での blow up とする．例外曲線を E とする．$K_{\tilde{S}}, (E.E)$ などを計算してみよう．以下 4 節での局所表示記号を用いることにする．このとき，S の 0 でない有理 2 形式は有理関数 $f \neq 0$ を用いて $\omega := f dx \wedge dy$ と表示できる．ω を $\tilde{S}$ に引き戻すことで $\tilde{S}$ の有理 2 形式 $p^*\omega$ ができる．ここで K_S の因子の代表元としては ω の因子を採用し，$K_{\tilde{S}}$ の因子の代表元には $p^*\omega$ の因子を採用することにする．p^*K_S と $K_{\tilde{S}} = \mathrm{div}(p^*\omega)$ を比べてみよう．p は P 上を除けば同型なので，食い違い $K_{\tilde{S}} - p^*K_S$ は E にしかないはずである．従って，4 節の座標系 $(U_1, (x, t)) \subset \tilde{S}, (U, (x, y)) \subset S$ に制限して調べれば十分である．(x, y) は U の座標系だったので，$\mathrm{div}(\omega)|U = \mathrm{div}(f)|U$ である．ゆえに，

$$p^*\mathrm{div}(\omega)|U_1 = p^*\mathrm{div}(f)|U_1 = \mathrm{div}(p^*f)|U_1$$

である．また，U_1 上では $y = xt$ だったから

$$\pi^*(\omega)|U_1 = (p^*f)dx \wedge d(xt)|U_1 = p^*f x dx \wedge dt|U_1$$

である．ここで，$E|U_1 = (x = 0)$ だった．従って，因子として

$$K_{\tilde{S}} = p^*K_S + E$$

となる．このように blow up すると上の標準因子は下の標準因子より例外因子ぶんだけ大きくなる．

次に $(E.E)$ を求めてみよう．$S \subset \mathbb{P}^N$（射影性の定義）だから，$\mathbb{P}^N$ の超平面 $\tilde{H} (\not\supset S)$ から S の因子 $H = \tilde{H} \cap S$（**超平面切断**）ができる．一つの超平面切断 H は P の近傍で $(x = 0)$ と一致するよう選び，もう一つの超平面切断 H' は P を通らないように選ぶ．blow up の局所表示から，$p^*H = H' + E, H' = (t = 0), E = (x = 0)$ である．(x, t) は U_1 における座標系だったので，H' と E は E の 1 点で横断的に交わる．ゆえに

$$(p^*H.E) = (H'.E) + (E.E) = 1 + (E.E)$$

である．他方，$H = H' + (f)(f \in \mathbb{C}(V))$ である．ゆえに $p^*H = p^*H' + (p^*f)$ であり，p^*H と p^*H' は $\tilde{S}$ においても線形同値である．従って

$$(p^*H.E) = (p^*H'.E) = 0$$

である．H' は P を通らないので，$p^*H' \cap E = \emptyset$ だからである．以上 2 式から

$(E.E) = -1$

がわかる．$(E.E)$ を E^2 と書けば，$E^2 = -1$ であり，E は虚数単位 $\sqrt{-1}$ に似ている．例外曲線は交点数においてもどこかミステリアスな曲線である．

詳細は省くが，添加公式と呼ばれる公式を用いると

$(K_{\tilde{S}}.E) = -1$

がわかる．交点数 $(K_{\tilde{S}}.E)$ が負であることが数値的極小モデル理論の1つの原点であり，高次元においてはより本質的となる．

一般に滑らかな射影曲面 S 上の曲線 E で $E \simeq \mathbb{P}^1$ かつ $(E.E) = -1$ をみたすものを**第一種例外曲線**という．blow up の例外曲線は第一種例外曲線である．第一種例外曲線を有しない滑らかな射影曲面のことを**古典的極小モデル**という．blow up の逆操作により，すべての滑らかな射影曲面は古典的極小モデルにできることを主張するのが次の Castelnouvo の定理である：

定理 6.1. *滑らかな射影曲面 S に第一種例外曲線 E があれば，E だけを blow up の逆操作により滑らかな射影曲面の点に収縮できる．すなわち，滑らかな射影曲面 $\overline{S}$ と全射正則双有理写像 $c : S \to \overline{S}$ で，$c(E) = \mathrm{Q}$ は1点，$S \setminus E \to \overline{S} \setminus \{\mathrm{Q}\}$ は同型となるものがある．また，次の意味で blow up の逆操作になっている：$p : S' \to \overline{S}$ を Q における $\overline{S}$ の blow up とするとき，$c^{-1} \circ p : S' \to S$ は双正則写像である．*

$b_2(\overline{S}) = b_2(S) - 1$ であり，$b_2(S)$ は自然数なので，定理の第一種例外曲線の収縮操作は有限回の後に終了し，古典的極小モデルに到達するのである．この定理は曲面の研究を古典的極小モデルの研究に帰着させる曲面論における最重要定理の一つである．曲面の（古典的）極小モデル S は，有理曲線族で覆われるものとすべての曲線 C に対し $(K_S.C) \geq 0$ であるもの（**数値的極小モデル**）の2タイプに大別され，さらに，数値的極小モデルでは，因子 mK_S（m は適当な正整数）に付随する有理写像が正則写像となり，像上標準的にファイバー付けされる（**幾何学的極小モデル**）．穏やかな特異点を許容した高次元化が現代双有理幾何学における主要な問題の一つである．3次元の場合は解決されている（川又雄二郎先生，宮岡洋一先生，森重文先生）．より高次元の場合の研究が現在活発である．現状は，名著『高次元代数多様体論』（川又雄二郎著，岩波書店）を参照されたい．

（おぎそ・けいじ，大阪大学大学院理学研究科）

Galois表現と整数論

三枝 洋一

1. はじめに

本稿では，現代の数論において盛んに研究されているGalois表現を題材にとり，なぜそのようなものを考えるのか，どのようなことが分かっているのかなどをできるだけ素朴な視点から論ずることで，数論における考え方の一端を探りたい．

2. 問題設定

以下の3つの比較的素朴な問題から始めよう．本稿を通して p は素数を表すものとする．

> **(A)** $x^2 \equiv 2 \pmod{p}$ となる整数 x は $\bmod p$ でいくつあるか？
>
> **(B)** $x^3 \equiv 2 \pmod{p}$ となる整数 x は $\bmod p$ でいくつあるか？
>
> **(C)** $y^2 + y \equiv x^3 - x^2 \pmod{p}$ となる整数の組 (x, y) は $\bmod p$ でいくつあるか？

代数の言葉を用いると，(A) は有限体 $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ において方程式 $x^2 - 2 = 0$ にいくつ解があるかという問題だと解釈できる．(B), (C) も同様である．

実際にやってみると，(A) については容易に答えが推測できると思う．$p = 2$ のとき1個，$p \equiv 1, 7 \pmod{8}$ のときは2個，$p \equiv 3, 5 \pmod{8}$ のときは0個となる．Gaussによる平方剰余の相互法則の一部として結果をご存知の方も多いだろう．一方, (B) や (C) についてはそれほど簡単な法則性は見つからない．特に，(B) は (A) と非常に似た形をしているにもかかわらず，p をある整数で割った余りを見ることでは解の個数を判定することができないのである．この差異は，方程式 $x^2 - 2 = 0$ と $x^3 - 2 = 0$ が異なる種類の対称性を有していることから生じるものである．次節では，このことについて見ていくことにする．

3. mod p での方程式と Galois 群

まず，方程式の対称性を記述する群である **Galois 群**について簡単に振り返っておく．$f(x)$ を有理数係数の n 次既約多項式とし，その複素数体の中での根を $\alpha_1, \ldots, \alpha_n$ とおく．有理数体 $\mathbb{Q}$ に $\alpha_1, \ldots, \alpha_n$ を添加した体を $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ と書き，$f(x)$ の最小分解体と呼ぶ．K の自己同型 $\sigma\colon K \to K$ 全体のなす群を $\mathrm{Gal}(K/\mathbb{Q})$ と書き，$K/\mathbb{Q}$ のGalois群，あるいは多項式 $f(x)$ のGalois群と呼ぶのであった．σ は根 $\alpha_1, \ldots, \alpha_n$ の置換を引き起こす．そのため，$\mathrm{Gal}(K/\mathbb{Q})$ は n 次対称群 S_n の部分群となる．$f(x) = x^2 - 2$ の場合は $\mathrm{Gal}(K/\mathbb{Q}) = S_2 = \mathbb{Z}/2\mathbb{Z}$ であり，$f(x) = x^3 - 2$ の場合は $\mathrm{Gal}(K/\mathbb{Q}) = S_3$ である．しかし，いつでも $\mathrm{Gal}(K/\mathbb{Q}) = S_n$ となるわけではない．例えば $f(x) = x^4 + x^3 + x^2 + x + 1$ のとき，$\zeta = e^{\frac{2\pi i}{5}}$ とおくと $\zeta, \zeta^2, \zeta^3, \zeta^4$ が $f(x)$ の4根を与える．σ は同型だから $\sigma(\zeta^i) = \sigma(\zeta)^i$ なので，ζ のうつる先を決めれば他の根のうつる先も決まってしまう．この

考察から, $\mathrm{Gal}(K/\mathbb{Q})$ の位数は4であり, S_4 の位数24とはほど遠いことが分かる. 上の例に垣間見えるように, Galois 群は, 根の間にどのくらい非自明な代数関係式があるかという情報を内包している.

Galois 群を用いて問題 (A), (B) を解釈したいのであるが, それにはもう少し準備が必要である. 整数係数のモニック多項式の根となるような複素数のことを**代数的整数**という. $f(x)$ および K を前述の通りとし, K に含まれる代数的整数全体を O_K と書く. $f(x) = x^2 - 2$ ならば $O_K = \mathbb{Z}[\sqrt{2}] = \mathbb{Z}[x]/(x^2 - 2)$ である. この環を「$\mathrm{mod}\, p$」して得られる環 $O_K/pO_K = \mathbb{F}_p[x]/(x^2-2)$ を考えてみよう. まず, x^2-2 が $\mathbb{F}_p$ 内に2根 a, b を持つ場合, $\mathbb{F}_p[x]$ において $x^2-2=(x-a)(x-b)$ と因数分解されるから, 中国剰余定理によって $O_K/pO_K = \mathbb{F}_p \times \mathbb{F}_p$ が分かる. 一方, x^2-2 が $\mathbb{F}_p[x]$ において既約な場合には, O_K/pO_K はこのように直積には分解せず, $\mathbb{F}_p$ の2次拡大体 $\mathbb{F}_{p^2}$ となる. 最後に, x^2-2 が $\mathbb{F}_p$ 内に重根を持つ場合（つまり $p=2$ の場合）には, O_K/pO_K は非自明な冪零元を持つ環 $\mathbb{F}_2[x]/(x^2)$ となる. これらの3種類の環は, p 乗写像 $\varphi_p \colon O_K/pO_K \to O_K/pO_K$ を見ることによって区別される（O_K/pO_K においては $p=0$ なので, $(a+b)^p = a^p + b^p$ となり p 乗写像が準同型になることに注意). $O_K/pO_K = \mathbb{F}_p \times \mathbb{F}_p$ ならば φ_p は恒等写像 id であるが, $O_K/pO_K = \mathbb{F}_{p^2}$ のときは $\varphi_p \neq \mathrm{id}, \varphi_p^2 = \mathrm{id}$ となる. これら2つの場合には φ_p は同型であるが, $p=2$ のときは φ_p は単射でないので同型でもない. 特に $p \neq 2$ の場合には, 次が分かったことになる：

$$x^2-2 \text{ が } \mathbb{F}_p \text{ 内に（2つの）根を持つ}$$
$$\iff \varphi_p \colon O_K/pO_K \to O_K/pO_K \text{ が id.}$$

ここまでは $f(x)=x^2-2$ としてきたが, O_K/pO_K 上の p 乗写像 φ_p は $f(x)$ が一般の場合にも問題なく定義される. φ_p が同型であるとき, $K/\mathbb{Q}$ は p で**不分岐**であるという. このとき, O_K/pO_K は互いに同型な $\mathbb{F}_p$ の拡大体いくつかの直積となる. 不分岐という言葉遣いは, Riemann 面の被覆との類似に由来するものである.

Galois 群の話に戻ろう. $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ とすると, σ は O_K を保つので, $\mathrm{mod}\, p$ をとることで環の同型 $\overline{\sigma} \colon O_K/pO_K \to O_K/pO_K$ が誘導される. これに対し, 次が成り立つ.

定理1 $K/\mathbb{Q}$ が p で不分岐であると仮定する. $O_K/pO_K = \mathbb{F}_{p^f} \times \cdots \times \mathbb{F}_{p^f}$ の直積因子を一つ固定すると, $\overline{\sigma}$ がその因子を保ち, かつその上で p 乗写像 φ_p と一致するような $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ が一意的に存在する.

定理中の σ を Frob_p と書き, p における **Frobenius 元**と呼ぶ. 直積因子の選び方を変えると Frob_p は $\mathrm{Gal}(K/\mathbb{Q})$ の中で共役な元に変わるので, Frob_p は共役類のみが well-defined である（したがって $\mathrm{Gal}(K/\mathbb{Q})$ がアーベル群ならば Frob_p 自体も well-defined). 先程の同値性と合わせると, $f(x)=x^2-2, p \neq 2$ のときには次が分かる：

$$x^2-2 \text{ が } \mathbb{F}_p \text{ 内に（2つの）根を持つ}$$
$$\iff \mathrm{Gal}(K/\mathbb{Q}) = S_2 \text{ 内で } \mathrm{Frob}_p = 1.$$

つまり, x^2-2 の $\mathbb{F}_p$ 内での根の様子を調べるという問題が, $\mathrm{Frob}_p \in \mathrm{Gal}(K/\mathbb{Q})$ がどのような元かという問題へと再定式化されたのである.

詳しい説明は省くが, $f(x)=x^3-2$ とすることで, 問題 (B) に対しても同様の言い換えが可能である. この場合, $p \neq 2,3$ のとき $K/\mathbb{Q}$ は p で不分岐となり, $\mathrm{Frob}_p \in \mathrm{Gal}(K/\mathbb{Q}) = S_3$ が共役を除いて定義される. Frob_p の共役類によって, x^3-2 の $\mathbb{F}_p$ 内での根の個数が以下のように決定できる：

$$\begin{cases} 3 \text{ 個} & (\mathrm{Frob}_p = 1), \\ 1 \text{ 個} & (\mathrm{Frob}_p \text{ は } (1\ 2) \text{ と共役}), \\ 0 \text{ 個} & (\mathrm{Frob}_p \text{ は } (1\ 2\ 3) \text{ と共役}). \end{cases}$$

これは, $\mathrm{Frob}_p \in S_3$ の3点集合への自然な作用（根の置換に対応する）の固定点の個数が $\mathbb{F}_p$ 内での根の個数となるということである.

では, $\mathrm{Frob}_p \in \mathrm{Gal}(K/\mathbb{Q})$ はどのようにして決定されるのだろうか. この問題がうまく解決できる場合として, **円分体**の場合が挙げられる. 整数 $m \geq 1$ に対し $\zeta_m = e^{\frac{2\pi i}{m}}$ とおき,

$f_m(x)=\prod_{1\le i\le m,(m,i)=1}(x-\zeta_m^i)$ を円分多項式と呼ぶ．これは x^m-1 を割り切る有理数係数多項式となる．例えば $f_5(x)$ は以前出てきた $x^4+x^3+x^2+x+1$ である．$f_m(x)$ の最小分解体を $\mathbb{Q}(\mu_m)$ と書く．こうして得られる体が円分体である．$m=5$ のときに説明したように，$\sigma\in\mathrm{Gal}(\mathbb{Q}(\mu_m)/\mathbb{Q})$ は $\sigma(\zeta_m)$ を決めると決まってしまう．$\sigma(\zeta_m)$ は ζ_m^i (i は m と互いに素) という形なので，σ に $i \bmod m$ を対応させることで単射群準同型 $\chi_m\colon \mathrm{Gal}(\mathbb{Q}(\mu_m)/\mathbb{Q})\hookrightarrow(\mathbb{Z}/m\mathbb{Z})^\times$ が得られる．これについて次が成り立つ．

定理 2 p と m が互いに素なとき，$\mathbb{Q}(\mu_m)/\mathbb{Q}$ は p で不分岐であり，$\chi_m(\mathrm{Frob}_p)=p \bmod m$ が成り立つ．特に χ_m は全単射である．

$f(x)=x^2-2$, $K=\mathbb{Q}(\sqrt{2})$ のとき，K は $\mathbb{Q}(\mu_8)$ に含まれる．実際，$\sqrt{2}=\zeta_8+\zeta_8^{-1}$ である．この式を使うと，$\mathrm{Frob}_p(\sqrt{2})=\zeta_8^p+\zeta_8^{-p}$ と計算できる．右辺は $p\equiv 1,7 \pmod 8$ のとき $\sqrt{2}$, $p\equiv 3,5 \pmod 8$ のとき $-\sqrt{2}$ となるので，$\mathrm{Frob}_p\in\mathrm{Gal}(K/\mathbb{Q})$ が 1 になることは $p\equiv 1,7 \pmod 8$ と同値であることが従う．

実は，$\mathrm{Gal}(K/\mathbb{Q})$ がアーベル群ならば K はある円分体 $\mathbb{Q}(\mu_m)$ に含まれることが知られている (**Kronecker–Weber の定理**)．このときにも上と全く同様の手順で，$\mathrm{Frob}_p\in\mathrm{Gal}(K/\mathbb{Q})$ がどのような元になるかを p を m で割った余りによって決定することができる．これが有理数体 $\mathbb{Q}$ に対する類体論の概要である．

一方，$f(x)=x^3-2$ の場合は $\mathrm{Gal}(K/\mathbb{Q})=S_3$ が非可換群であるため，上記の議論を適用することができない．これが問題 (A) と問題 (B) の本質的な差異だったのである．

4. Galois 表現による記述

これまでは，方程式 $f(x)=0$ に合わせて考える体 K を変えていたが，これらをまとめて考えた方が便利である．代数的数，すなわち有理数係数多項式の根となる複素数全体を $\overline{\mathbb{Q}}$ と書く．これは複素数体の部分体であり，前節で考えた体 K を全て含んでいる．自己同型 $\sigma\colon\overline{\mathbb{Q}}\to\overline{\mathbb{Q}}$ 全体を $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ あるいは $\Gamma_{\mathbb{Q}}$ と書き，$\mathbb{Q}$ の**絶対 Galois 群**と呼ぶ．これは無限群である．K を $\mathbb{Q}$ の有限次 Galois 拡大 (すなわち，有理数係数既約多項式の最小分解体として書ける体) とするとき，自己同型を制限することによって全射 $\Gamma_{\mathbb{Q}}\to\mathrm{Gal}(K/\mathbb{Q})$ が得られる．これの核を単位元の基本近傍とするような位相 (**Krull 位相**) を入れることで，$\Gamma_{\mathbb{Q}}$ はコンパクトな位相群となる．Galois 表現とは，この位相群 $\Gamma_{\mathbb{Q}}$ の連続表現のことである．

$\Gamma_{\mathbb{Q}}$ における Frobenius 元の定義はやや込み入っている．代数的整数全体のなす環を $\overline{\mathbb{Z}}$ と書き，$\overline{\mathbb{Z}}$ の素イデアル $\mathfrak{p}$ で $\mathfrak{p}\cap\mathbb{Z}=p\mathbb{Z}$ となるものを固定する．$\sigma\in\Gamma_{\mathbb{Q}}$ は $\overline{\mathbb{Z}}$ を保つので，$\mathfrak{p}$ の σ による像 $\sigma(\mathfrak{p})$ を考えることができる．$\sigma(\mathfrak{p})=\mathfrak{p}$ となる σ 全体を $D_{\mathfrak{p}}$ と書き，$\mathfrak{p}$ における**分解群**と呼ぶ．$\sigma\in D_{\mathfrak{p}}$ は $\overline{\mathbb{Z}}/\mathfrak{p}=\overline{\mathbb{F}}_p$ の自己同型 $\overline{\sigma}$ を誘導するが，これが恒等写像となる σ 全体を $I_{\mathfrak{p}}$ と書き，$\mathfrak{p}$ における**惰性群**と呼ぶ．$\overline{\sigma}$ が $\overline{\mathbb{Z}}/\mathfrak{p}$ の p 乗写像となるような $\sigma\in D_{\mathfrak{p}}$ を Frob_p と書き，Frobenius 元と呼ぶ．この元は一意的ではなく，$I_{\mathfrak{p}}$ による剰余類を除いてしか決まらない．また，$\mathfrak{p}$ をとりかえると $D_{\mathfrak{p}}, I_{\mathfrak{p}}$ は $\Gamma_{\mathbb{Q}}$ 内で共役な部分群に変わるので，さらに任意性があることになる．

$\mathbb{Q}$ の有限次 Galois 拡大 K に対し，$K/\mathbb{Q}$ が p で不分岐であることと $\Gamma_{\mathbb{Q}}\to\mathrm{Gal}(K/\mathbb{Q})$ による $I_{\mathfrak{p}}$ の像が自明になることは同値である．この意味で，$I_{\mathfrak{p}}$ は p での分岐の度合いを測っている．$K/\mathbb{Q}$ が p で不分岐ならば，$\mathrm{Frob}_p\in\Gamma_{\mathbb{Q}}$ の $\mathrm{Gal}(K/\mathbb{Q})$ における像は先に定義した Frobenius 元と一致する．

前節の考察を Galois 表現を用いて捉え直してみよう．まず，問題 (A) に対応する場合を考える．

$$\Gamma_{\mathbb{Q}}\to\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})=\{\pm1\}\subset\mathbb{C}^\times=\mathrm{GL}_1(\mathbb{C})$$

によって，1 次元連続表現 $\rho_{\mathrm{A}}\colon\Gamma_{\mathbb{Q}}\to\mathrm{GL}_1(\mathbb{C})$ が得られる．$p\neq 2$ ならば $\rho_{\mathrm{A}}(I_{\mathfrak{p}})=1$ であるから (このような表現を p で不分岐であるという)，$\rho_{\mathrm{A}}(\mathrm{Frob}_p)$ の共役類は well-defined であり，したがってそのトレース $\mathrm{Tr}\,\rho_{\mathrm{A}}(\mathrm{Frob}_p)$ も well-defined

である．さらに，次が成り立っている：

$$(x^2-2 \text{ の } \mathbb{F}_p \text{ での根の個数}) = 1+\operatorname{Tr}\rho_{\mathrm{A}}(\mathrm{Frob}_p).$$

問題 (B) はどうだろうか．K を x^3-2 の最小分解体とすると，$\mathrm{Gal}(K/\mathbb{Q})=S_3$ は 3 次元ベクトル空間 $\mathbb{C}^3$ に成分の置換で作用する．この 3 次元表現は自明表現を部分表現に持ち，それによる商は S_3 の唯一の既約 2 次元表現となる．これを st と書き，合成 $\varGamma_{\mathbb{Q}} \to \mathrm{Gal}(K/\mathbb{Q}) = S_3 \xrightarrow{\mathrm{st}} \mathrm{GL}_2(\mathbb{C})$ で得られる 2 次元 Galois 表現を ρ_{B} とおく．ρ_{B} は $p \neq 2,3$ で不分岐であり，次が成り立つ：

$$(x^3-2 \text{ の } \mathbb{F}_p \text{ での根の個数}) = 1+\operatorname{Tr}\rho_{\mathrm{B}}(\mathrm{Frob}_p).$$

こうして Galois 表現の言葉を用いることで，問題 (A), (B) を統一的に記述することができた．(A) が 1 次元表現の問題であるのに対し，(B) は 2 次元表現の問題となり，その難しさの差が明確になったともいえる．

ここで，これまで触れてこなかった問題 (C) を思い出そう．方程式 $y^2+y=x^3-x^2$ には変数が 2 つあるので，最小分解体をとって $\mathbb{Q}$ の有限次 Galois 拡大を作ることはできない．また，Galois 表現 $\rho\colon \varGamma_{\mathbb{Q}} \to \mathrm{GL}_n(\mathbb{C})$ のトレース $\operatorname{Tr}\rho(\mathrm{Frob}_p)$ を用いて $y^2+y=x^3-x^2$ の $\mathbb{F}_p$ における解の個数を記述することも実は不可能である．しかし，Galois 表現を $\mathbb{C}$ 上で考えるのでなく，素数 ℓ を固定し，ℓ 進数体 $\mathbb{Q}_\ell$ の代数閉包 $\overline{\mathbb{Q}}_\ell$ 上で考えれば，解の個数が記述できるのである．

定理 3　2 次元 Galois 表現 $\rho_{\mathrm{C}}\colon \varGamma_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{Q}}_\ell)$ で次を満たすものが存在する：$p \neq 11, \ell$ ならば ρ_{C} は p において不分岐であり，

$$(y^2+y=x^3-x^2 \text{ の解 } (x,y)\in\mathbb{F}_p^2 \text{ の個数}) = p-\operatorname{Tr}\rho_{\mathrm{C}}(\mathrm{Frob}_p).$$

$\mathbb{C}$ と $\overline{\mathbb{Q}}_\ell$ は体としては同型であるが，位相は異なる．Galois 表現には連続性が課されるため，どちらの体の上で表現を考えるかによって違いが出てくる．$\mathbb{C}$ は連結だが，$\overline{\mathbb{Q}}_\ell$ は全不連結である．$\varGamma_{\mathbb{Q}}$ の位相も全不連結であるため，似た位相を持つ $\overline{\mathbb{Q}}_\ell$ のほうが Galois 表現が豊富である．$\mathbb{C}$ 上の Galois 表現は必ず像が有限になるが，$\overline{\mathbb{Q}}_\ell$ の方はそうではない（実際，ρ_{C} の像は無限群である）．$\overline{\mathbb{Q}}_\ell$ 上で Galois 表現を考えることを強調するときには，**ℓ 進 Galois 表現**という．これに対し，$\mathbb{C}$ 上の Galois 表現は **Artin 表現**と呼ばれる．体の同型 $\mathbb{C} \cong \overline{\mathbb{Q}}_\ell$ を固定することで，Artin 表現は ℓ 進 Galois 表現とみなすことができるが，逆はそうではない．

5. Galois 表現とエタールコホモロジー

定理 3 における ρ_{C} の構成は，ρ_{A} や ρ_{B} のように単純ではない．(A) や (B) の方程式が 0 次元の空間を定めるのに対し，(C) の方程式 $y^2+y=x^3-x^2$ は代数曲線を定めることがその原因である．この代数曲線に無限遠点を付け加えて射影代数曲線としたものを E と書く．これは**楕円曲線**の一例となっている．目標は，E の $\mathbb{F}_p$ 有理点の集合 $E(\mathbb{F}_p)$ の元の個数 $\#E(\mathbb{F}_p)$ を記述する ℓ 進 Galois 表現を構成することである．

設定を一般化して，$\mathbb{Q}$ 上滑らかな射影代数多様体 X に対して ℓ 進 Galois 表現を構成するという問題を考えよう．これは **ℓ 進エタールコホモロジー** $H^i_{\text{ét}}(X_{\overline{\mathbb{Q}}}, \overline{\mathbb{Q}}_\ell)$ を考えることによって達成される（$X_{\overline{\mathbb{Q}}}$ は X を底変換によって $\overline{\mathbb{Q}}$ 上の代数多様体とみなしたもの）．位相空間に対するコホモロジー（**Betti コホモロジー**）はトポロジーにおける強力な道具であるが，その定義の方法の一つに定数層を係数とする層係数コホモロジーを考えるというものがある．エタールコホモロジーは，この定義が代数多様体の枠組みの中でうまく機能するように適切な修正を行うことによって得られるコホモロジーである．$H^i_{\text{ét}}(X_{\overline{\mathbb{Q}}}, \overline{\mathbb{Q}}_\ell)$ は X を複素多様体と見たもの $X(\mathbb{C})$ の Betti コホモロジー $H^i_{\mathrm{Betti}}(X(\mathbb{C}), \mathbb{Q})$ に $\overline{\mathbb{Q}}_\ell$ をテンソルしたものと同型である．こう書くと Betti コホモロジーとエタールコホモロジーはあまり変わりがないように見えるが，両者の最大の違いは，$H^i_{\text{ét}}(X_{\overline{\mathbb{Q}}}, \overline{\mathbb{Q}}_\ell)$ は $\varGamma_{\mathbb{Q}}$ の作用を持つという点にある．この作用によって，各次数 i に対し，ℓ 進 Galois 表現 $\rho^i_X\colon \varGamma_{\mathbb{Q}} \to \mathrm{GL}(H^i_{\text{ét}}(X_{\overline{\mathbb{Q}}}, \overline{\mathbb{Q}}_\ell))$ が得られる．これについて，以下が知られている．

定理 4 p を ℓ と異なる素数とし，X が p においてよい還元を持つとする（これは概ね，X の定義方程式を $\bmod p$ して得られる $\mathbb{F}_p$ 上の代数多様体 X_p が特異点を持たないことを指す）．このとき，次が成り立つ．

1. ρ_X^i は p において不分岐である．
2. 整数 $n \geq 1$ に対し，
$$\sum_{i=0}^{2\dim X} (-1)^i \operatorname{Tr} \rho_X^i(\mathrm{Frob}_p^{-n}) = \# X_p(\mathbb{F}_{p^n}).$$
3. $\rho_X^i(\mathrm{Frob}_p^{-1})$ の固有値は代数的数であり，その全ての共役元の複素絶対値は $p^{i/2}$ に等しい．

3 はいわゆる **Weil 予想**（Deligne の純性定理）である．2 と 3 を組み合わせると，各 i に対する $\operatorname{Tr} \rho_X^i(\mathrm{Frob}_p^{-1})$ を $\{\# X_p(\mathbb{F}_{p^n})\}_{n\geq 1}$ から計算することができる．Weil 予想はしばしば Riemann 予想の類似であることが強調されるが，このようにコホモロジーの次数を分離する力を持った実用的な定理でもある．

$X = E$ の場合を考えよう．$E(\mathbb{C})$ は複素トーラスであり，位相空間としては $S^1 \times S^1$ と同相であるから，$\rho_E^0, \rho_E^1, \rho_E^2$ はそれぞれ 1 次元，2 次元，1 次元の表現であり，$i \geq 3$ ならば $\rho_E^i = 0$ である．E は $p \neq 11$ においてよい還元を持つから，ρ_E^i は $p \neq 11, \ell$ において不分岐となる．$p \neq 11, \ell$ のとき，$\operatorname{Tr} \rho_E^0(\mathrm{Frob}_p^{-1}) = 1$, $\operatorname{Tr} \rho_E^2(\mathrm{Frob}_p^{-1}) = p$ であることが比較的容易に分かるから，定理 4 の 2 より，$\operatorname{Tr} \rho_E^1(\mathrm{Frob}_p^{-1}) = 1 + p - \# E_p(\mathbb{F}_p)$ となる．したがって，ρ_{C} を ρ_E^1 の双対表現とすれば定理 3 の条件を満たす 2 次元 Galois 表現が得られる*1)．

実は，(A) や (B) の場合にも定理 4 は有効である．例えば X を方程式 $x^3 - 2 = 0$ で定まる $\mathbb{Q}$ 上の 0 次元射影代数多様体とすると，X が p でよい還元を持つことは $\mathbb{Q}(\sqrt[3]{2})$ が p で不分岐であること，すなわち $p \neq 2, 3$ と同値であり，このとき X_p は方程式 $x^3 - 2 = 0$ で定まる $\mathbb{F}_p$ 上の 0 次元射影代数多様体となる．$X(\mathbb{C})$ は 3 点からなる空間であるから，ρ_X^0 は 3 次元表現であり，$i \geq 1$ に対し $\rho_X^i = 0$ となる．したがって $p \neq 2, 3, \ell$ のとき $\operatorname{Tr} \rho_X^0(\mathrm{Frob}_p^{-1}) = \# X_p(\mathbb{F}_p)$ である．右辺は $x^3 - 2$ の $\mathbb{F}_p$ での根の個数に他ならない．ρ_X^0 は自明表現を部分表現に持ち，それによる商の双対表現をとると前節で構成した ρ_{B} が得られる．このように $\mathbb{Q}$ の有限次拡大体を幾何学的な対象とみなすというのは 20 世紀以降の整数論における重要な考え方の一つである．

楕円曲線 $E\colon y^2 + y = x^3 - x^2$ の 1 次エタールコホモロジーから得られた Galois 表現 ρ_{C} は既約であることが証明できるが，一般に射影代数多様体 X から生まれる Galois 表現が既約であるとは限らない（実際，上の例 $X\colon x^3 - 2 = 0$ では ρ_X^0 は可約である）．そのようなときには，X の**代数的対応**によってエタールコホモロジーの一部を切り取るということがよく行われる．ここでの代数的対応とは，$X \times X$ の余次元 $\dim X$ の閉部分多様体の形式的な $\overline{\mathbb{Q}}_\ell$ 線型結合のことである．例えば，X から X への射はグラフを考えることで代数的対応の一種とみなせる．代数的対応 Γ は $H_{\mathrm{\acute{e}t}}^i(X_{\overline{\mathbb{Q}}}, \overline{\mathbb{Q}}_\ell)$ の自己線型写像 Γ^* を引き起こす．これは $\Gamma_{\mathbb{Q}}$ の作用と可換なので，像 $\operatorname{Im} \Gamma^*$ は ρ_X^i の部分表現となる．特に $(\Gamma^*)^2 = \Gamma^*$ のとき，$\operatorname{Im} \Gamma^*$ は ρ_X^i の直和因子であり，この場合には定理 4 と似た形で Galois 表現 $\operatorname{Im} \Gamma^*$ を幾何学的に調べることができる．X とこのような代数的対応 Γ の組は**モチーフ**と呼ばれている．モチーフは，Galois 表現を生み出すいわば構成単位である．

本節の最後に，本題とは少し外れるが，ℓ 進 Galois 表現がどのくらい代数多様体，あるいはモチーフを区別できるかについて補足しておこう．X, X' が楕円曲線の場合には，ρ_X^1 と $\rho_{X'}^1$ が同型であることと X と X' が同種であることの同値性が証明されている（アーベル多様体の Tate 予想，Faltings の定理）．また，一般の射影代数多様体に対する Tate 予想を仮定すると，2 つのモチーフが同じ ℓ 進 Galois 表現を生むならば，それらは（適切な意味で）同型であることが帰結される．Tate 予想は現状では解決の見通しがない，極めて難しい未解決問題ではあるが，部分的な結果もあり，Galois

*1) 定理 3 の式と 1 だけずれているように見えるのは，無限遠点を付け加えているためである．

表現に関わる研究者の間では高い信憑性をもって受け入れられているようである．モチーフは全てのよいコホモロジーを生み出すおおもと（普遍的なコホモロジー理論）であると考えられており，それがエタールコホモロジーによって完全に把握されてしまうというのはいささか不思議ではあるが，それだけエタールコホモロジーや ℓ 進 Galois 表現が本質的な対象であるということなのだと思う．

6. Galois 表現と保型形式

エタールコホモロジーによって，(A), (B), (C) のような方程式の問題を Galois 表現の問題へと書き直す統一的な方法が得られた．しかし，まだ問題 (B), (C) そのものへの解答が得られたわけではない．ここ半世紀の整数論においては，これらの種類の問題を**保型形式**と結び付けることで理解することを一つの目標としてきた．保型形式について簡単に思い出しておこう．$w \geq 1$, $N \geq 1$ を整数とし，$\mathrm{SL}_2(\mathbb{Z})$ の部分群 $\Gamma_1(N)$ を

$$\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \;\middle|\; c \equiv 0, d \equiv 1 \pmod N\right\}$$

で定める．上半平面 $\mathfrak{H} = \{z \in \mathbb{C} \mid \mathrm{Im}\, z > 0\}$ 上の正則関数 f が重さ w，レベル N の保型形式であるとは，$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_1(N)$ に関する対称性

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^w f(z)$$

を有することをいう*2)．特に $f(z+1) = f(z)$ であるから，$q = e^{2\pi i z}$ とおくと $f(z) = \sum_{n=0}^{\infty} a_n q^n$ と展開できる（**q 展開**）．問題 (B), (C) と関わるのは，それぞれ以下の保型形式である：

$$f_{\mathrm{B}}(z) = q \prod_{n=1}^{\infty} (1 - q^{6n})(1 - q^{18n}),$$

$$f_{\mathrm{C}}(z) = q \prod_{n=1}^{\infty} (1 - q^{n})^2(1 - q^{11n})^2.$$

$f_{\mathrm{B}}(z)$ の重さは 1，レベルは 108 であり，$f_{\mathrm{C}}(z)$ の重さは 2，レベルは 11 である．これらの保型形式は q 展開の定数項が 0 であるという特徴を持っており，**尖点的保型形式**と呼ばれている*3)．

$f_{\mathrm{B}}(z)$ と ρ_{B}，$f_{\mathrm{C}}(z)$ と ρ_{C} の間にはそれぞれ以下のような関係がある．

定理 5 **1.** $f_{\mathrm{B}}(z) = \sum_{n=1}^{\infty} a_n q^n$ と書くと，$p \neq 2, 3$ に対し $a_p = \mathrm{Tr}\, \rho_{\mathrm{B}}(\mathrm{Frob}_p)$ が成り立つ．

2. $f_{\mathrm{C}}(z) = \sum_{n=1}^{\infty} b_n q^n$ と書くと，$p \neq 11, \ell$ に対し $b_p = \mathrm{Tr}\, \rho_{\mathrm{C}}(\mathrm{Frob}_p)$ が成り立つ．

つまり，$f_{\mathrm{B}}(z)$, $f_{\mathrm{C}}(z)$ の q 展開の p 番目の係数に問題 (B), (C) の答えが現れるということである．例えば，$f_{\mathrm{B}}(z)$ の q 展開における q^{691} の係数 a_{691} は 2 となるから，$x^3 - 2$ は $\mathbb{F}_{691}$ 内に 3 個の根を持つことが分かる．

2 次元 ℓ 進 Galois 表現が保型形式と関係するという現象は定理 5 に限ったことではなく，ずっと一般的な状況で成立すると期待されている．

期待 1 2 次元既約 ℓ 進 Galois 表現と尖点的保型形式の間には自然な対応がある*4)．Galois 表現 ρ と保型形式 $f(z) = \sum_{n=1}^{\infty} a_n q^n$ が対応するとき，$f(z)$ のレベルと素な素数 $p \neq \ell$ において ρ は不分岐で $a_p = \mathrm{Tr}\, \rho(\mathrm{Frob}_p)$ が成り立つ．

保型形式 $f(z)$ に対して Galois 表現を構成する方向については，比較的古くから研究が進んでおり，現在では理論が完成している．そのアイデアを，保型形式 $f_{\mathrm{C}}(z)$ を例にとって簡単に説明しよう．重さ 2，レベル 11 の保型形式は，Riemann 面 $Y_1(11) = \mathfrak{H}/\Gamma_1(11)$ 上の正則微分形式と解釈できる．さらに，保型形式の尖点性は，対応する微分形式が $Y_1(11)$ のコンパクト化 $X_1(11)$ 上に正則に延長されることと同値である．この $X_1(11)$ は $\mathbb{Q}$ 上定義される射影代数曲線であることが知られている（**モジュラー曲線**）．重さ 2，レベル 11 の

*2) 正確には，カスプでの正則性も課す必要がある．

*3) 正確には，全てのカスプでの値が 0 であることを要求する．

*4) 実際は，Galois 表現の方には「ほとんど全ての素数において不分岐，ℓ で de Rham，$\det \rho(c) = -1$ ($c \in \Gamma_{\mathbb{Q}}$ は複素共役)」という条件を，保型形式の方には「正規化された Hecke 固有新形式」という条件を課す必要がある．Galois 表現に対する条件は後述の定理 6 や定理 7 にも現れる．

尖点的保型形式の空間が1次元であることから，$X_1(11)$ は種数1の代数曲線，すなわち楕円曲線となることが分かる．その1次エタールコホモロジー $\rho^1_{X_1(11)}$ の双対が $f_{\mathrm{C}}(z)$ に対応するGalois表現を与える．実は，$X_1(11)$ は以前考えた楕円曲線 $E\colon y^2+y=x^3-x^2$ と一致するので，ここでの構成は前節における ρ_{C} の構成に他ならない．

重さ2でレベル N が一般の場合にも，同様にモジュラー曲線 $X_1(N)$ のエタールコホモロジーを考えることで保型形式に対応するGalois表現を構成できる．ただし，一般には保型形式の空間が1次元とは限らないので，Hecke対応と呼ばれる代数的対応を用いて $H^1_{\text{ét}}(X_1(N)_{\overline{\mathbb{Q}}},\overline{\mathbb{Q}}_\ell)$ の一部を切り取る必要がある（ここにモチーフの考え方が現れる）．重さが3以上の場合にも，モジュラー曲線の係数付き交叉コホモロジーを考えることで類似の構成が可能である．

重さが1であるときは，上のような幾何学的な構成は知られていない．この場合には，$f(z)$ と $\mathrm{mod}\,\ell$ で合同な q 展開を持つ尖点的保型形式 $g(z)$ で重さが2以上のものをうまくとり[*5]，$g(z)$ に対応するGalois表現 ρ' を考える．適切な素数 ℓ に対し，ρ' を $\mathrm{mod}\,\ell$ して得られる $\overline{\mathbb{F}}_\ell$ 上のGalois表現は $\overline{\mathbb{Q}}_\ell$ 上のGalois表現で像が有限なもの ρ に持ち上がり，この ρ が $f(z)$ に対応するGalois表現となる（Deligne–Serreの構成．この場合 ρ はArtin表現である）．こうした代数的操作は，Galois群やモチーフを見ているだけでは捉えることができない．Galois表現の柔軟さを感じさせられる．

一方，Galois表現に保型形式を対応させる方向の研究の歴史は比較的新しいが，Taylor–Wilesによる志村–谷山予想の部分的解決を突破口として，今世紀に入ってから爆発的に研究が進展し，期待1の解決にあと少しのところまで迫っている状況にある．現時点で得られている有力な結果を2つ挙げておこう．

定理6（強Artin予想）　ρ を2次元既約Artin表現とし，$\det\rho(c)=-1$ と仮定する（$c\in\Gamma_{\mathbb{Q}}$ は複素共役）．このとき，重さ1の尖点的保型形式で ρ に対応するものが存在する．

定理7（Fontaine–Mazur予想の一部）　ρ を2次元既約 ℓ 進Galois表現とし，ほとんど全ての素数において不分岐，ℓ でde Rham, $\det\rho(c)=-1$ と仮定する．$\ell\neq 2$ かつ ℓ におけるHodge–Tate重さ a,b が相異なると仮定し，さらに ρ を $\mathrm{mod}\,\ell$ して得られる表現 $\overline{\rho}$ に少し技術的な条件をつける．

このとき，重さ $|a-b|+1$ の尖点的保型形式で ρ の指標による捻りに対応するものが存在する．

定理6はKhare–WintenbergerによってSerre予想の解決の系として得られた(2009)．定理7は，Breuil, Colmezらによる p 進ラングランズ対応とモジュラー曲線の完備エタールコホモロジーの理論を組み合わせることで，Emertonによって証明された[*6]．定理7の条件に出てくる「de Rham」や「Hodge–Tate重さ」についてはここでは説明することができないが，**p 進Hodge理論**における基本的な概念であるということのみ述べておく．

7. おわりに

本稿ではGalois表現が2次元である場合に限って解説を行った．この場合が最も現象が見やすく，また分かっていることが多いためである．より次元の高いGalois表現を考える際には，現在の整数論における一つの柱である**保型表現論**が不可欠となる．他にも様々な魅力的なアイデアが現れるが，それについては別の機会に論ずることとしたい．

近年，この分野の研究は目覚ましい発展を遂げている．筆者が数学を始めたのはFermat予想が解決された少し後であるが，その頃と比べても隔世の感がある．Galois表現というものに対する印象もだいぶ変わってきたように思う．今後の進展が楽しみである．

（みえだ・よういち，東京大学大学院数理科学研究科）

*5）例えば，重さ $4(\ell-1)$，定数項1のEisenstein級数との積をとればよい．

*6）証明の書かれた論文はまだプレプリントである．

名著に親しむ

——特集から広がる読書案内——

梶　元

代数幾何まなびはじめ

理工学部数学科に進学した頃は，自分が数学者になるとは考えてもみなかったし，まさか代数幾何を専門にするとは想像したこともなかった．数学科を卒業後は物理学科に学士編入し，理論物理学者となって宇宙の構造やブラックホールを研究する‘計画’だった．

それには微分幾何が重要なので，研究室配属後（学部3年後期）は名著と名高い Kobayashi–Nomizu, “Foundations of Differential Geometry” (Wiley) で勉強する予定だった．しかし，微分幾何の先生を訪ねてみると「そのテキストでは（セミナーは）しません」とあっさり却下されてしまった．当時，Penrose による複素幾何を用いた宇宙論などの研究の存在を知ったので「では複素幾何でもいいかな」ということで，今思えばかなり安直に代数幾何の先生を訪ねて「Griffiths–Harris, “Principles of Algebraic Geometry” (John Wiley & Sons) でセミナーをしていただけませんか」とお願いした．しかし，これまた却下．結局，友人が希望した代数的代数幾何の入門書，**[H]** Hartshorne, “Algebraic Geometry” (Springer GTM52) がテキストとなった．先生からは，**[AM]** Atiyah–MacDonald, “Introduction to Commutative Algebra” (Addison-Wesley) の知識が必要なので，夏休み中に読んでみたらどうかと勧められた．

[AM] は可換環論の古典的名著として有名である．でも代数は得意でも好きでもなかった．‘代数嫌い’といってもいいだろう．さらに，当初の‘計画’からするともうかなり脱線している．これは困ったことになったと思った．しかし **[AM]** を読み始めるとその意外な面白さに不覚にも感動してしまった．邦訳すれば書名は「可換代数入門」であるが内容はまさに『幾何』である．「そんなの，信じられない！」という方はまず，第1章の練習問題で‘*Spec* の呪文’をマスターしてほしい．**[AM]** は，「*Spec!*」と唱えながら読めば脳内に幾何的実体が立ち上がるヴァーチャル『飛び出す絵本』である．

[AM] を読了後 **[H]** を読み始めたが，本文冒頭からほんの数行を読み進むのでさえ莫大な時間がかかった．こんなに分厚い本を読み通すのに一体，どれくらいの時間がかかるのだろうかと，本を眼の前にして愕然とした覚えがある．それでも練習問題を解きつつ何とか読み進めていくと，豊富に鏤められた例や練習問題，そして具体的計算の面白さに魅了されて，代数幾何の世界にどんどん引き込まれていった．砂を噛むような学習効率重視のテキストとは一線を画する（それでも先生は「この本は，‘高速道路’みたいなものだな」と，おっしゃっていた）．「入門書として内容が不十分だ」，「重要な命題が練習問題になっている」などのご批判はたしかに耳にする．しかし，では誰がこれを超える魅力的な代数的代数幾何の入門書を，しかもこれほどコンパクトに書くことができるだろうか．

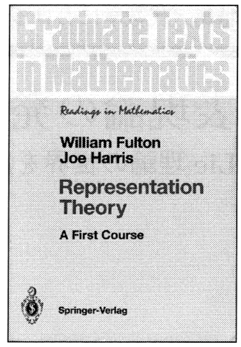
セミナーでの発表は練習問題の解答に専念することになった．授業期間中は週1回，春休み夏休み期間中は週2回のペースで毎回，ネタ（学生側の解いてきた問題）が尽きるまで，5–6時間は続いた．だいたい昼頃から始めていたが，終了が夜の9時過ぎになることもあった．問題が目の前で先に，誰かに解かれてしまうのは癪に障るので，自分が発表予定の問題だけでなく，人の分までセミナーまでに全部解いてやろうと躍起になっていた．そうして2年間ほど宮崎誓氏ら友人と競い合うようにして無我夢中で練習問題を解いていた．まさしく字句のとおりで，自分が射影多様体になる夢，はたまた，代数幾何学の命題自体になる夢を見るようになった．「えっ！　それって，どういう夢？」と思われるかも知れない．でも紙面の制限もあるので，詳細はまた別の機会に書くことにしよう．今思い起こせば，若さゆえの勢いに任せた‘筋トレ’みたいなもので，ただただ数学だけに没頭し夢のような時間を過ごしていたことに気づく．

名著 **[H]** に出会ったため学部4年の頃には，当初の壮大な‘計画’はどこへやら，完全に代数幾何の虜である．優秀な良き友人たちに恵まれたのはもちろんのこと，われわれ学生に膨大な時間と労力を費やしてくださった恩師有馬哲先生の存在が不可欠だったことはいうまでもない．有馬先生にはいくら感謝してもしきれない．

（かじ・はじめ，早稲田大学理工学術院）

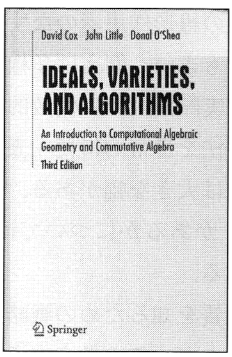
Representation Theory

W. Fulton, J. Harris 著, xv+551p., Springer, 2004



ルート系の森の探検

有限群および代数群の表現論に関する専門書．代数群やその表現論などを理解したくなり，名著といわれる Humphreys のリー代数の表現論や線形代数群をテキストとして，以前，友人たちを巻き込んで集中セミナーなど開いてみたりした．しかし，読み方が悪いのか理解力に問題があるのか（多分，両方ですな），論理を辿ることはできても，解った気には全然ならなかった．ところがこの本を読んでみると，ルート系の森の中を歩き回って探検している気分になり，感覚的にもルート系がしっくりときた．それまで頭の中に無秩序な感じで乱雑に散らばっていた断片的理解がきれいに繋がり，もやもやとしていた何かがさーっと晴れ渡る感じだった．多分，Humphreys 先生の本での修行の御利益もあるのだろう．もちろん本書のほうが優れているという話ではない．単に読み手との相性の問題である．蛇足だが，本書および Baston–Eastwood, "The Penrose Transform" (Oxford) に出会わなければ，等質射影多様体関係の論文は書けなかったと思う．



Ideals, Varieties, and Algorithms

David A. Cox, J. Little, D. O'Shea 著, 3rd ed., xv+553p., Springer, 2007

グレブナー基底で遊ぼう！

もはや古典ともいうべきグレブナー基底に関する入門書．初学者に不親切な教科書が世に少なくないと私は感じるが，この本を読んでみて，教科書とは，こうあるべきなのか！ こういう風に書けばいいのか！と改めて感じ入った．ところで，この機会に思い出したのは著者の 1 人，Don O'Shea との出会いである．1985 年アメリカ数学会夏季研究集会で学生寮のアパートを 1 週間シェアした．どこの馬の骨かわからない，英語をほとんど話せないヤセっぽちの東洋人（その頃は私もヤセていたのだ）に随分と親切に接してくれた．例えば週末には，彼の車で映画館（"Cocoon" がかかっていた）に連れていってくれたりした．当時のその他諸々の出来事を思い起こせば，彼の関わった著作に，数学専門書に不慣れな初学者への暖かい心遣いや細やかな配慮が満ち溢れていることは当然で，何ら不思議ではない．素晴らしい入門書である．

表現論の発想

Lie 理論の世界を超えて

有木　進

1. はじめに

線形空間 A に加法・乗法が定義されていて，結合法則・加法の交換法則・分配法則などをみたしているとき，線形空間 A を**代数**というのであった．n 次正方行列の全体はもっとも基本的な代数の例である．$1 \in A$ を A の乗法の単位元とする．行列代数の場合乗法の単位元とは単位行列に他ならない．以下，写像はすべて線形写像とする．

定義 1　A から行列代数への写像 ρ であって，$\rho(1)$ が単位行列かつ任意の $x, y \in A$ に対して

$$\rho(x+y) = \rho(x) + \rho(y), \quad \rho(xy) = \rho(x)\rho(y)$$

をみたすものを A の**表現**と呼ぶ．本稿では $\rho(A)$ の作用する線形空間も表現と呼ぶことにしよう．

ある代数 A を理解したいとしよう．A 自体の構造を調べる，例えばイデアルを計算する，などがまず思い浮かぶかもしれない．しかし，実際には実行するのが大変であることも多い．その場合に代数 A の性質を A の表現を通じて理解しようとする．そして表現を研究するのが表現論である．表現を通じて A の構造を理解できるもっとも簡単な例を挙げよう．

定理 1（Maschke, Artin–Wedderburn）　G を有限群，標数 p の代数閉体 $\mathbf{F}$ 上定義された G の群代数を A とする．G の位数（集合 G の元の個数）が p で割り切れないとし，G のすべての既約表現の次元がわかっているとする．$d_1, \ldots, d_s$ が既約表現の次元だとすると，A は行列代数の直和 $\bigoplus_{i=1}^{s} \mathbf{F}^{d_i \times d_i}$ に同型である．

表現論が扱うのは有限次元表現に限るわけではない．無限次元線形空間上の線形作用素のなす代数への代数準同型を考えてもよい．例えば多様体上の関数空間などである．実際，純粋に代数的な表現論から幾何や解析の手法を日常的に使う表現論まで表現論の研究分野には大きな幅がある．どんな研究者コミュニティーがあるかについては，次節でより具体的に説明する．

研究対象である代数の性質を知るための戦略として表現を研究すると言ったが，この考え方自体は決して表現論特有のものではない．例えばある多様体を理解したいと思うとき，その上の関数（またはより一般に層の大域切断）のなす線形空間を調べるであろう．我々は層の圏の代わりに表現の圏を扱うという点だけが違いともいえる．しかも，多様体が群作用を許せばこれらの空間は群の表現を与えるので必然的に表現論が応用されることになるから，どこまでが表現論独特の発想でどこからがそうではないかも定かではない．表現論の発想とは何だろう．圏論的な研究に軸足があって，三角圏の研究が多く行われているのは確かである．Artin 代数の表現論でも Lie 理論の表現論でも代数幾何的な手法が多くみられるのも特徴である．しかし，この傾向は他分野，例えば数論，におい

ても同様なのであり，表現論特有というよりは現代数学に共通する特徴であろう．代数や多様体のもつある性質が実は加群や連接層から作られる圏のみから決まる性質であることが判明すれば，同じ圏をもつ別の代数や多様体を調べてもよい．つまり，一見かなり見かけの異なる別の代数での表現論の計算が，実はもとの代数の性質を教えてくれる．この種の発想が現代数学のいたるところで使われているのである．

実際，編集部から今回お題をいただいていろいろ考えてみたが，技術的には何でも使うので他分野の手法も重宝するし，発想も表現論独特で他にはないものを見つけるのは難しい．その結果，表現論の発想とは表現という対象へ持つ愛着，つまり**表現が第一**という発想ではないかと思うようになった．もちろん，表現論が素粒子論や数理物理，はたまた数論等で応用されるのをうれしいと思う表現論研究者も多いと思う．しかし他分野に行けば表現論は主役ではなく，研究の背景にある問題意識はあくまでも物理や数論固有のものであり，自分もおもしろいと思えるかは別問題である．表現論研究者は，応用に関係なく表現論が好きなのである．そして，数理的事象を見るたびに表現論的記述があり得るかを気にし，もし記述方法が複数あれば表現論的記述を優先するのである．私はこの心の持ち方を表現論の発想と呼ぶこととしたい．実際，次節で述べるように，表現論内部の各分野を眺めてみればその発想の出発点は様々であって，それぞれが何かしら表現論以外の分野と共通の発想・技術を使っているのである．このことに気づいてみれば，表現論研究者を表現論研究者たらしめているのは，個々の研究で使う発想・技術と言うよりは，表現論の設定で研究するという姿勢ではないかと思うのは自然であろう．

本稿では，表現論的発想の具体例として行列の組 (A, B) を座標変換して (PAQ, PBQ) と変えるときどういう標準形に持っていけるかを考える．答えは**Kronecker 標準形**と呼ばれる有名なものであるが，その証明を文献 2) の XII 章と文献 3) の VIII 章の 2 つで比較すればその違いに驚くであろう．昔は存在しなかった表現論という分野の出現が証明の発想自体を変えたのである．他にも，対称群（より一般に Weyl 群）の既約表現が，Springer 表現という全く別の発想で構成された例もある．これは数論や位相幾何学における技術の進歩を表現論に応用したのであるから，表現論独自の発想とはいえないが，表現論第一と思う心を持った者が他分野での進歩を見るからこそ応用が可能になったのだと思う．しかも，この技術は Lie 理論における他の多くの表現論にも成功裏に応用され，表現論の世界で深く尊敬される分野を生み出したのである．これは表現論の発想が偉いのであろうか，それとも技術が偉いのであろうか．どちらにせよ，表現論の発想でこの技術を使いこなし，深い結果を生んでいった偉大な研究者たちが偉いことは間違いないのではあるが．

以下では，まず表現論分野を概観し，次に Kronecker 標準形の導出を例に表現論の発想を見る．また，旧来の Hecke 代数や Schur 代数の表現論を Fock 空間の圏化という目を通じて見ることで生まれた新しい表現論—箙 Hecke 代数の表現論—について最後に少しだけ触れたい．

2. 研究から見た表現論分野概観

表現論の分野のリストアップから話を始めよう．アメリカ数学会のデータベース MSC2010（Mathematics Subject Classification）を見ると

- **16Gxx** Representation theory of rings and algebras,
- **16Hxx** Algebras and orders,
- **16Txx** Hopf algebras, quantum groups and related topics,
- **17Bxx** Lie algebras and Lie superalgebras,
- **20Cxx** Representation theory of groups,
- **20Gxx** Linear algebraic groups and related topics,
- **47–xx** Operator theory,

などが目につく．最後の xx はその分類番号の中の細目の番号で，例を挙げると 20C08 は Hecke

algebras and their representations である．

最後の Operator theory は違う世界の表現論である．代数的な部分もないわけではないが，代数からは縁遠いので考えないことにしよう．また，実 Lie 群の表現論も代数的な表現論が多く含まれているのであるが，代数群の表現論に含めることにする．

さて，この結果を見ると，表現論は可換環や Artin 代数の表現論を研究するコミュニティー，低次元トポロジーにも関係が深い Hopf 代数のコミュニティー，有限群のモジュラー表現論のコミュニティー，また Lie 代数の研究と代数群や Lie 群の研究を行う Lie 理論のコミュニティーから成り立っていることがわかる．実際，研究者が帰属意識をもつ研究集会もコミュニティーに応じて異なることが多い．日本では可換環や Artin 代数の表現論がしっかりとした一分野を形成している．この分野では代数の表現のなす圏が出発点である．

例 1　行列代数 $\mathbf{F}^{n\times n}$ の有限次元表現は n 次元ベクトルのなす自然表現 $V = \mathbf{F}^n$ の直和と同型なものがすべてである．代数 A の有限次元表現のなす圏とは，A の任意の表現 X, Y に対して，A の作用と可換な線形写像 $X \to Y$ の全体を射の集合 $\mathrm{Hom}_A(X, Y)$ と称して記憶しておくものであるから，行列代数の有限次元表現のなす圏は有限次元線形空間のなす圏と同じ（圏同値）である．実際，自然表現 V を 1 次元線形空間に対応させれば同一視できる．

つまり，この分野の発想は表現のもつ個性のうち表現の次元等は一切無視する価値観から始まる．すると，すべての既約表現は 1 次元だとしても一般性を失わず，さらに，すべての代数の表現論は有向グラフの表現論に帰着できてしまう．その結果，表現のなす圏についてより深い議論ができるのである．

近年は加群圏から作られる種々の圏の部分圏に関する研究が盛んであり，圏自体の研究が大きな割合を占めるというのがこの分野の特徴である．Hopf 代数の表現論のコミュニティーでも極めて圏論的な研究が行われている．どちらも分野の育成に筑波大学が大きな役割を演じた．

他方，有限群のモジュラー表現論においては既約表現の次元は大事な個性の一つである．しかも対称群の場合でさえまだ既約表現の次元を決定できていないのである．日本においては散在型有限単純群を愛する人々がいるが，表現論研究者にとっては，有限個しかないので計算機プロジェクトに適当な題材という点に価値がある．私自身は，無限系列からなりかつ自然な幾何的対象と結びつく古典型の Lie 型有限群のモジュラー表現論がもっとも重要な研究対象だと考えている．実際，古典型は Deligne–Lusztig 理論を駆使する分野であり，Lie 理論に属する代数群分野の表現論研究者の研究対象でもある．他方で，有限群のモジュラー表現論は Lie 理論の枠を超えて有限群一般に成り立つ種々の予想が存在する独自の世界でもある．任意の有限群 G に対し，G のモジュラー既約表現の同型類の個数を与える予想が存在するが，分野外の数学者はほとんど知らないのではなかろうか．数学科の 3 年次に一言でも触れてほしいものである．この予想は Alperin の重み予想と呼ばれる．G の p-部分群 Q と射影既約 $N_G(Q)/Q$-加群 S の組 (Q, S) を重みと呼ぶ．p-正則共役類とは違い，Lie 理論の最高重みの拡張概念になっている．重み予想は重みの共役類とモジュラー既約表現の同型類が同じ個数であることを主張する．散文的な感想を書いたが，他にも Broué 可換不足群予想など導来圏同値の研究も盛んな分野である．

次に Lie 理論のコミュニティーを見てみよう．この分野では，Lie 代数の表現論か代数群・Lie 群の表現論かに関わらず

- 既約表現の同型類の分類，
- 既約表現の構成法，
- 余積をもつ代数ならばテンソル積の分解，
- 部分代数の表現への分岐則

を調べるのが常道である．つまり，Lie 理論の表現論研究者の発想は上記問題をどう解決するかを目指すところから始まる．この点だけでも Artin 代数の表現論分野とはかなり違うことが見て取れ

る．また，既約表現の次元も Lie 理論の表現論では大事な個性であるが無限次元表現を扱うこともよくある．affine 型 Lie 代数は数理物理との関係もあってとくに詳しく研究されている．Artin 代数の表現論分野と同様，圏論的な議論もよく使うが Lie 理論のコミュニティーでは幾何的な対象のなす圏をよく用い，表現論の発想も幾何的な発想が先に立つ場合が多い．閑話休題：京都では歴史的な経緯から Lie 理論は解析学の一分野であり，東京と京都を中心に Lie 理論の表現論が盛んな時期があったが，今は過渡期に入っていると言えるだろう．今の京都では頂点代数の表現論や幾何的表現論が華やかである．日本における Lie 理論コミュニティーの研究の対象をひとことで言えば，量子群・Lie 代数・Lie 群・p 進代数群とその関連分野ということになるだろうか．

ここまで表現論分野を概観してきて改めて思うことであるが，発想とは自らのもつ技術に相当程度支配されるようである．それぞれのコミュニティーで重要な Auslander–Reiten 理論，Brauer の主定理，Deligne–Lusztig 理論などを学ぶとそれぞれの理論の発想の癖も一緒に習得している．それが問題意識の違いにも現れてくるのであろう．

3. 人から見た表現論分野概観

Artin 代数と Lie 理論の表現論は同じ表現論と言っても研究者コミュニティーの相互交流が少ないのが現状である．いろいろな場面でそれを実感するのであるが，ごく最近では 2013 年に名古屋で開催された山形邦夫先生 65 歳記念国際研究集会での Skowroński 先生のスピーチであった．Lie 理論の研究者が全くいない集まりを日本の表現論コミュニティーのすべてであるかのように表現するスピーチに大いに違和感を感じたのである．同じ表現論であるから開発された技術を一方の分野でしか使わないのはもったいないと感じるので，もっとお互いの技術を使っていきたいものであるが，そのためには問題意識にも共通項が出てくるようなよい研究対象が必要かもしれない．上記で概観したように，技術面だけではなく研究の対象自体がかなり異なっているのが現状であるが，cluster 代数のように多くの表現論分野に関係して成功している例もあるので悲観したものでもない．

他にも代数的組合せ論や数理物理の表現論が存在するが，上記分野と重なる部分もあるのでここでは説明を省略する．

4. Kronecker 標準形

表現論がどんな世界かわかったところで次に表現論の視点がどう違うかを考えよう．とくに線形代数の問題などを表現論の問題として見るのは，表現論の土俵に載せるかどうかで解決の道筋が違ってくることがわかるよい例である．

線形代数の問題を表現論の問題として見るとはどういうことか，まず Jordan 標準形の例を挙げて説明しよう．正方行列 A が与えられたとする．このとき，一変数多項式環 $\mathbf{C}[x]$ から行列代数への代数準同型を $f(x) \mapsto f(A)$ で定義すると $\mathbf{C}[x]$ の表現が得られる．この見方によれば，Jordan 標準形を求める問題は多項式環 $\mathbf{C}[x]$ の表現の分類問題と言い換えられる．これだけだと単に物の見方を変えただけと思うかもしれないが，いったん表現論になれば表現論の技術が適用可能になり，全く別の理論展開が可能になるのが要点である．改めて，発想は自らのもつ技術に相当程度支配される，と感じる．

A が n 次ならば n 次元数ベクトルのなす線形空間を V とし，表現を $\rho : \mathbf{C}[x] \to \mathrm{End}_{\mathbf{C}}(V)$ と考えよう．V を $\mathbf{C}[x]$-加群とも呼ぶ．ここで，V の**射影分解**を考えると次の完全系列を得る．

$$0 \to \mathbf{C}[x]^n \to \mathbf{C}[x]^n \to V \to 0.$$

$\mathbf{C}[x]^n \to \mathbf{C}[x]^n$ は多項式成分ベクトルに多項式成分行列 $xI - A$ を掛ける写像である．ゆえに，$xI-A$ を行基本変形と列基本変形で標準形に持っていくことにより V の標準形が得られる．実際，V の標準形を求めた結果として行列 A の Jordan 標準形が得られるのである．私が学生の頃に線形

代数の教科書の定番だった齋藤正彦著『線型代数入門』(東京大学出版会) ではこの導出方法を射影分解等の基礎知識なしに理解できる形で書いていた．数学者は足場を隠す，の典型例かもしれないが，あとで代数学に触れてその本来の姿を理解するときには若干の感動があるだろう．ただ，数学科のカリキュラムで主イデアル整域を習うときは環論が前面に出て，表現論的な見方を強調することはないように思う．Jordan 標準形の理論を一変数多項式環の表現論として教えてほしいと思うが，なかなか難しいかもしれない．ちなみに，頂点が 1 つで頂点から自分自身へのループが 1 本書かれた有向グラフを **Jordan quiver** と呼ぶ．一変数多項式環とは Jordan quiver の道代数に他ならず，我々は有向グラフの表現論をやっているのである．

さて, 考え方は同様であるがもう少し複雑な Kronecker 標準形の導出に移ろう．

m 行 n 列の行列 A, B が与えられたとする．A と B に同じ基本変形を施していくとき, (A,B) をどういう形の標準形に持っていけるだろうか．基本変形は行基本変形と列基本変形の両方を使ってよい．つまり，P と Q を m 次と n 次の可逆正方行列として $(A,B)\mapsto(PAQ,PBQ)$ という操作を許すとき，(A,B) をどういう標準形に持っていけるか，という問題を考える．

文献 2) の XII 章で紹介されている方法は，pencil と呼ばれる多項式成分行列 $A+xB$ を扱い標準形に持っていこうとするものである．他方，文献 3) の VIII 章で紹介されている方法はまず問題を表現論の問題として定式化する．

2 点を頂点にもち一方の頂点から他方の頂点に 2 本の有向辺を引いた有向グラフを **Kronecker quiver** と呼ぶ．頂点に 1, 2 と名前を付け，頂点 2 から頂点 1 に引いた有向辺に α,β と名前を付けよう．この有向グラフの道代数とは，e_1,e_2,α,β を基底とする 4 次元代数であって乗積表が表 1 で与えられる代数のことである．行列を用いて次のように具体的に表すこともできる．

表 1　Kronecker 代数の乗積表.

ab	$b=e_1$	$b=e_2$	$b=\alpha$	$b=\beta$
$a=e_1$	e_1	0	α	β
$a=e_2$	0	e_2	0	0
$a=\alpha$	0	α	0	0
$a=\beta$	0	β	0	0

$$\left\{\begin{pmatrix} a & c & d \\ 0 & b & 0 \\ 0 & 0 & b \end{pmatrix} \middle|\ a,b,c,d\in\mathbf{C}\right\}.$$

道代数の表現は有向辺に線形写像を載せた表示で表すのが便利である．今は，α と β に行列 A と B を載せたものになる．行列代数への代数準同型写像を具体的に書けば，

$$e_1\mapsto\begin{pmatrix} I_m & 0 \\ 0 & 0 \end{pmatrix},\quad e_2\mapsto\begin{pmatrix} 0 & 0 \\ 0 & I_n \end{pmatrix},$$
$$\alpha\mapsto\begin{pmatrix} 0 & A \\ 0 & 0 \end{pmatrix},\quad \beta\mapsto\begin{pmatrix} 0 & B \\ 0 & 0 \end{pmatrix}$$

となる．乗積表をみたし表現を与えていることは簡単に確認できるであろう．この読み換えにより，問題は Kronecker 代数の表現の標準形を求める問題に置き換わる．この場面で使う表現論の技術は Auslander–Reiten 理論である．$\mathbf{C}[x]$ の表現論のとき Jordan 細胞と呼んだ表現は**直既約表現**と呼ばれる表現の標準形であり，表現は直既約表現の直和になっているから，以下でも直既約表現の標準形を求めればよい．直既約表現（の同型類）は **Auslander–Reiten quiver** という有向グラフの頂点になっていて，$\boldsymbol{A_1^{(1)}}$ **型ルート系**の正ルートに合わせて 3 種類の部分，postprojective, regular, preinjective 成分に分かれる．ルートには実ルートと虚ルートの区別があり，regular 成分以外の成分は実ルートに対応していて，各ルートに対し直既約表現が一つずつ対応している．postprojective 成分の場合は $m=n+1$ で，I_n を n 次単位行列とすると

$$A=\begin{pmatrix} I_n \\ 0 \end{pmatrix},\quad B=\begin{pmatrix} 0 \\ I_n \end{pmatrix}$$

が対応する標準形である．preinjective 成分では行と列を転置した標準形が対応する．

regular 成分は値として ∞ を取ることを許す変数 λ を持つ．Jordan 標準形が固有値と組成列の長さで決まる標準形を持つように，$m=n=1$ の直既約表現 $A=(1), B=(\lambda)$ があり，変数 λ の値ごとに，この表現を対角成分にもち組成列の長さで決まる直既約表現の標準形が存在する．ただし，$\lambda=\infty$ のときは $A=(0), B=(1)$ を用いる約束とする．

用語などわからない点も多いと思うが，雰囲気だけでも味わっていただけたであろうか．pencil の標準形という考え方ではなく，表現論の基礎理論の一つを常識とすれば別の議論によって容易に Kronecker 標準形が得られる，という事実を知っていただくだけで十分だと思う．

5. 円分箙 Hecke 代数

Hecke 代数とは対称群（またはより一般に Coxeter 群）の群代数の関係式に変数を入れて変形したものである．ある圏の Grothendieck 群として Hecke 代数を実現する理論は幾何的表現論に多く現れる．ここでは量子群の可積分最高重み加群をある代数の加群圏の Grothendieck 群として実現することを考える．このような考え方，つまり線形空間を圏で置き換え，線形写像を完全関手で置き換え，もとの線形空間と線形写像を圏と関手の影として理解する考え方を**圏化** (categorification) という．

今の場合，量子群の圏化の試みから箙 Hecke 代数が発見され，Khovanov–Lauda により円分箙 Hecke 代数という代数の研究が提案されたのである．さて，数理解析研究所の一時代を築いた京都学派の仕事により Fock 空間は Kac–Moody Lie 代数の表現論の枠組みで取り扱うことができるが，円分箙 Hecke 代数の直和は Fock 空間の中で真空が生成する既約部分加群の圏化を与えている．初見ではその基本関係式にぎょっとするかもしれないが，上で述べたように必然性があって生まれてきた代数なので研究に値する興味深い代数である．私は最近，この代数を理解するべくかなりの時間を注いでいる．技術的には量子群や結晶基底の Lie 理論，Fock 空間の表現論，Artin 代数の表現論の種々の定理が使われ，また他の研究者の研究でも組合せ論的表現論から幾何的表現論に至るまで幅広い技術が登場し，表現論のデパートといった趣がある．まだまだ知名度もなく，応用も限られた代数であるが，興味のある読者は論文を検索するなどされたい．圏論的分岐則など発想がおもしろい論文も現れている．

そういえば昔数学会秋季年会で講演したとき，Fock 空間の Kashiwara–Lusztig 標準基底は物理的に何か意味があるだろうか，と質問したことがある．数学が何でも物理に現れるというのは期待しすぎであるが，よい数学の多くが物理に現れるのもまた事実であるのでいつまでも気になっている．

6. 最後に

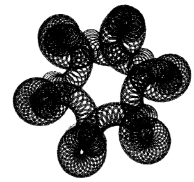
私はこれだけ広く深く育った表現論分野を横断的に知っている表現論プロパーの研究者が多く育つことを希望している．本特集号を手に取った読者の中からそのような志向性を持った若者が現れるとうれしい．入門書として文献 1) を挙げておく．

参考文献

1) 堀田良之，『加群十話—代数学入門』，朝倉書店，1988.
2) F.R. Gantmacher, *The Theory of Matrices vols.I and II*, New York, Chelsea, 1959.
3) M. Auslander, I. Reiten and S.O. Smalø, *Representation Theory of Artin Algebras*, Cambridge studies in advanced mathematics **36**, CUP, 1995.

（ありき・すすむ，大阪大学大学院情報科学研究科）

微分方程式とガロア理論



原岡　喜重

1. 求積法

ガロア理論は，2 次方程式，3 次方程式といった代数方程式の解の複雑さを測る美しい理論であった．同じようなことが微分方程式でもできないだろうか．

17 世紀に微分法とニュートン力学が誕生して，物理現象は微分方程式で記述されるようになった．例えばバネによる振動である単振動は

$$x'' = -\omega^2 x$$

という微分方程式で表される．ここで ω は正の定数．この微分方程式を解くと，

$$x(t) = A\sin(\omega t + \phi)$$

が得られる．A と ϕ は微分方程式を解く過程で現れた積分定数である．解が三角関数で表されたことにより，運動の様子が完全に把握できることになった（図 1）．

太陽と地球のように互いに万有引力を及ぼし合う 2 つの物体の運動を調べることを 2 体問題という．2 体問題についてもその運動は微分方程式で表され，計算は少し複雑になるが楕円が解曲線として現れることを明示的に記述できる．これは惑星は楕円軌道を描くというケプラーの第一法則を，ニュートン力学から導いたことになる．

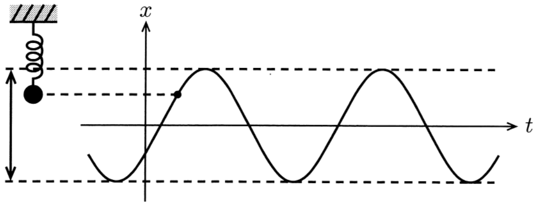


図 1　バネによる振動．

このように様々な重要な微分方程式が「解けて」，その解を見て運動を把握することができたため，いかにして微分方程式を解くかということが大きなテーマとなった．オイラー，ラグランジュといった一流の数学者たちが，競うように微分方程式の解法を編み出したのである．そのような解法の総体を**求積法**という．

例えば，最も基本的な変数分離形の方程式に対する求積法は次のような解法である．微分方程式が

$$\frac{dy}{dx} = f(x)g(y)$$

という形をしているとき変数分離形という．これを

$$\frac{dy}{g(y)} = f(x)\,dx$$

と書き，両辺を積分することで

$$\int \frac{dy}{g(y)} = \int f(x)\,dx$$

が得られる．両辺の不定積分をそれぞれ $G(y)$, $F(x)$ とすると，

$$G(y) = F(x) + C$$

となって，未知関数 $y(x)$ の陰関数表示が得られることになる．

このような技法が集積され，ちょうど2次方程式，3次方程式，4次方程式の解の公式が発見されて次は5次方程式の解の公式だ，と人々が思っていたように，微分方程式についてもそれぞれに解の公式を見つけようとしていた時期があったように思われる．

2. 微分方程式と解

19世紀はいろいろな意味で数学が大きな変貌を遂げた時代である．例えばガロア，リーマンが現れたのが19世紀．本稿との関係でいうと，微分方程式とは何か，その解となるのは関数だがそもそも関数とは何か，さらには関数の独立変数と値が動く領域である実数とは何か，という根源的なことについて深い省察がなされ，数学的対象をきっちりと考えるための基盤ができあがった．この新しい認識の下で微分方程式を定式化しよう．

独立変数を x，未知関数を $y(x)$ とおく．微分方程式とは，未知関数 y およびその（高階）導関数 $y', y'', \ldots, y^{(n)}$ についての方程式であり，$n+2$ 変数関数 $F(x, y_0, y_1, \ldots, y_n)$ を用いて

$$F(x, y, y', \ldots, y^{(n)}) = 0 \qquad \text{(E)}$$

の形に表されるものである（正確に言うとこれは単独高階型の常微分方程式というもので，未知関数を増やして方程式も増やした連立型，独立変数を増やした偏微分方程式も考えられる）．微分方程式 (E) の解 $y(x)$ とは n 回微分可能な関数で (E) をみたすもののことだが，相手は関数なので定義域が問題となる．したがって微分方程式の解を考えるときには，まず区間 I があり，I で定義された n 回微分可能な関数 $y(x)$ があって，各 $x \in I$ に対し $(x, y(x), y'(x), \ldots, y^{(n)}(x))$ が F の定義域に入っていることが前提となる．

さて19世紀の数学は，微分方程式 (E) の解を求めようなどという牧歌的な話ではなく，そもそも (E) に解は存在するのかという深刻なことを問うた．そして例えば F が連続であれば解が存在する，というような基本的な結果が得られたのである．コーシー，ペアノ，リプシッツなど，微分方程式の解の存在と一意性の定理に名前が出てくる人々は，みな19世紀の人である．

このような認識に立つと，微分方程式の解を明示的に求めるというのは絶望的に難しい問題であることがわかる．何しろ任意の微分可能な関数は何らかの微分方程式の解となるのだから．したがって解が明示的に求められていない状態で，（微分方程式を用いて）解の挙動を調べることが必要になる．これは現代の解析学の中心的なテーマであり，健全な方向である．一方，中には解ける微分方程式もあるのだから，微分方程式を見て解けるかどうかを判別したい，という問題も自然である．この問題を追及するのが，微分方程式のガロア理論である．

3. ピカール・ヴェシオ理論

微分方程式 (E) を見て，それが解けるかどうかを判別するという問題を考えよう．F が全く一般では手が出ないので，F の形を限定する．最も扱いやすいのは，F が $y, y', \ldots, y^{(n)}$ に関して線形になっている場合である．すなわち

$$y^{(n)} + p_1(x) y^{(n-1)} + \cdots + p_n(x) y = 0 \quad \text{(L)}$$

という微分方程式を考える．(L) を**線形常微分方程式**という．線形常微分方程式の著しい特徴は，解の定数係数線形結合がまた解になる，すなわち解の全体が線形空間をなす（この線形空間の次元は，微分方程式の階数と同じ n である）ということと，解は係数に現れる関数 $p_1(x), \ldots, p_n(x)$ が連続である区間でくまなく定義されるということである．したがって解ごとに定義域を考える煩わしさがない．

さて微分方程式 (L) が「解ける」ということの意味を確定しなくてはならない．例えば求積法により解が求まることをもって解けると定義したいと考える．ガロアの偉大な仕事の1つは，体（ガロアの言葉では rationnelle）とその拡大の概念を見出したことである．そのおかげで，（代数）方程

式が解けるということを，体の拡大の列

$$K_0 \subset K_1 \subset \cdots \subset K_m \qquad \text{(K)}$$

で，各 K_i/K_{i-1} は小さな拡大で，解が K_m に入っているようなものが存在すること，と定式化することができた．微分方程式についても，この定式化をそっくりいただくことができる．体としては微分が定義されるような微分体というものを考える必要があるが，あとは全く同じである．微分体 K_0 は微分方程式 (L) の係数 $p_1(x), \ldots, p_n(x)$ が属するように取る．拡大 K_i/K_{i-1} が小さいということをしかるべく定義さえすれば，解が K_m に入っていることをもって（その基準で）微分方程式が解ける，という風に定義できるのである．拡大 K_i/K_{i-1} が小さいということを，K_i が，K_{i-1} の元の不定積分や不定積分の指数関数や K_{i-1} の元を係数とする代数方程式の解を K_{i-1} に添加することで得られる，と定義するとき，K_m/K_0 を一般リウビル拡大という．これは (L) が求積法で解けるということのガロア理論的な定式化である．

ここで例を見てみよう．次の 2 つの微分方程式は求積法で解けるだろうか？

$$y'' - 2xy' + 4y = 0, \qquad \text{(He)}$$

$$y'' + xy = 0. \qquad \text{(A)}$$

(He) はエルミートの微分方程式（のパラメーターを特殊化したもの），(A) はエアリーの微分方程式と呼ばれる．見かけ上 (A) のほうが簡単に見えるが，(A) は求積法で解けず (He) が解けるのである．(He) が解けることは実際に解いてみればわかる．まず $y_1(x) = 2x^2 - 1$ が解となることが直接確かめられる．2 つ目の解 $y_2(x)$ は，$y_2 = y_1 z$ とおいて (He) の y のところに代入すると

$$\frac{z''}{z'} = 2x - \frac{8x}{2x^2 - 1}$$

が得られるので，これを積分することで

$$y_2(x) = (2x^2 - 1) \int \frac{e^{x^2}}{(2x^2 - 1)^2}\, dx$$

と求積できる．一方 (A) が解けないことを示すには，ガロア理論を必要とする．

線形常微分方程式に対するガロア理論はピカール，ヴェシオらによって作られた．微分体の拡大という概念があるのだから，あとはその拡大に対するガロア群を定めればよい．L/K を微分体の拡大とするとき，そのガロア群 $\mathrm{Gal}(L/K)$ は

$$\mathrm{Gal}(L/K) = \{\sigma : L \xrightarrow{\sim} L \mid \sigma(a) = a \ (\forall a \in K)\}$$

と定めるのが常道である．さてそれでは，K を微分方程式 (L) の係数 $p_1(x), \ldots, p_n(x)$ が属する微分体，L を K に (L) のすべての解を添加して得られる K の微分拡大体とするとき，そのガロア群 $\mathrm{Gal}(L/K)$ は何者だろうか．$\sigma \in \mathrm{Gal}(L/K)$ が K の元を動かさない L の微分自己同型であることから，(L) の両辺に σ を作用させた結果，

$$(\sigma(y))^{(n)} + p_1(x)(\sigma(y))^{(n-1)} + \cdots + p_n(x)\sigma(y) = 0$$

が得られることがわかるであろう．これにより，$\sigma(y)$ はまた微分方程式 (L) の解となる．すなわちガロア群の元は，(L) の解を (L) の解にうつす変換である．(L) の解全体は線形空間 V をなすので，その基底 $y_1, y_2, \ldots, y_n$ を取ることができ，これらの σ による像 $\sigma(y_1), \sigma(y_2), \ldots, \sigma(y_n)$ はまた V の基底となる．したがって σ に対して V の基底変換を与える行列 $A_\sigma \in \mathrm{GL}(n, C)$ が定まる．ここで C は K の定数体（微分して 0 となる K の元の全体）である．こうして $\mathrm{Gal}(L/K)$ は $\mathrm{GL}(n, C)$ の部分群 G として表現されるのである．G は代数群となることが示される．

さてピカール・ヴェシオ理論の美しい結果の 1 つに，L/K が一般リウビル拡大であることと G の単位元の連結成分が可解群であることが同値という定理がある．したがって G を求めることができれば，微分方程式 (L) が求積法で解けるかどうかが判定できるのである．ところが G を求めるのは実は大変難しい問題で，ここにピカール・ヴェシオ理論の限界がある．ガロア群 G を求めることについてほとんど唯一と思われる有効な方法は，(L) のモノドロミー群を用いるものである．

それについて説明しよう．

微分方程式 (L) の係数はすべて有理関数であるとして，$K=\mathbb{C}(x)$ とした場合を考える．各 i について有理関数 $p_i(x)$ の極の位数が高々 i のとき，その極は (L) の**確定特異点**と呼ばれるものになり，そこでは解が高々多項式程度の発散しかしないことが示される．∞ も込めて確定特異点しか持たない微分方程式を**フックス型**という．例えば

$$y'-\frac{a}{x}y=0$$

という微分方程式はフックス型である．これの解は $y(x)=x^a$ およびその定数倍である．x を複素変数とすると，

$$x^a=e^{a\log x}=e^{a(\log|x|+\sqrt{-1}\arg x)}$$

であるから，x が 0 のまわりを 1 周すると $\arg x$ が 2π 増えることにより，関数の値が $e^{2\pi\sqrt{-1}a}$ 倍になる（図 2）．このとき $x=0$ を x^a の**分岐点**という．このような解の多価性がフックス型微分方程式の本質である．

この多価性を一般に定式化しよう．(L) をフックス型とし，その確定特異点を $a_0,a_1,\ldots,a_p$ とする．x_0 をどの a_j とも異なる点として，x_0 の単連結近傍 U において定義される解空間の基底

$$\mathcal{Y}(x)=(y_1(x),\ldots,y_n(x))$$

を取る．$K=\mathbb{C}(x)$ に $y_1,\ldots,y_n$ を添加した微分体を L とする．γ を x_0 を基点とする $X=\mathbb{P}^1\setminus\{a_0,\ldots,a_p\}$ 内の閉曲線とすると，$\mathcal{Y}(x)$ の γ に沿った解析接続の結果 $\gamma_*\mathcal{Y}(x)$ はまた U における線形独立な解となる．したがってそれらは $y_1,\ldots,y_n$ の線形結合となるので，行列 M_γ を用いて

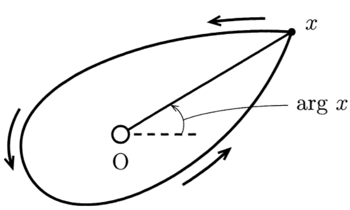


図 2　$\arg x$ の変化．

$$\gamma_*\mathcal{Y}(x)=\mathcal{Y}(x)M_\gamma$$

と表される．対応 $\gamma\mapsto M_\gamma$ は基本群の表現

$$\rho:\pi_1(X,x_0)\to \mathrm{GL}(n,\mathbb{C})$$

を定める．これを**モノドロミー表現**といい，その像を**モノドロミー群**という．解析接続は四則演算や微分と可換で，また有理関数は解析接続で不変なので，γ に沿った解析接続は L の K 上の自己同型，すなわち $\mathrm{Gal}(L/K)$ の元を定める．このことから，モノドロミー群はガロア群の部分群であることがわかる．実は次の事実が成り立つ．

定理　フックス型微分方程式においては，モノドロミー群のザリスキ閉包がガロア群となる[1)]．

集合 A のザリスキ閉包とは，A を含む最小の代数多様体を指す．この定理は，モノドロミー群が大きい，すなわち解の多価性が激しいと，解の超越性が高いということを定量的に述べたものである．モノドロミー群がわかればガロア群が求められることになるが，モノドロミー群を求めるのはまた難しい問題である．ただし方程式によってはモノドロミー群を明示的に求められることがあるので，この定理は有用である．

フックス型ではない不確定特異点を持つ微分方程式についても，モノドロミー群にストークス行列を付け加えた一般化モノドロミー群を考えると，そのザリスキ閉包がガロア群となることが示されている[2)]（ストークス行列というのは，不確定特異点における形式解と真の解の対応をつけるときに現れる行列である）．エアリーの微分方程式 (A) については一般化モノドロミー群を求めることができ，そのザリスキ閉包が可解群ではないことが示されるので，求積法では解けないことがわかる．

4. パンルベ方程式

19 世紀の終わりから 20 世紀のはじめにかけて，微分方程式を解くということに関して別の大きな出来事があった．パンルベ方程式の発見である．

単振動の微分方程式のように，解が三角関数や

指数関数で表せたときには，我々は微分方程式が解けたと感じる．それは三角関数や指数関数の挙動は完全に把握できるので，解の挙動もどこまでも追跡することができるからである．そうすると，これら初等関数以外にも挙動が把握できる関数を見つければ，その関数で書ける解を持つ微分方程式は「解ける」ことになるであろう．すなわち新しい「良い」関数の発見は，解ける微分方程式を増やすことにつながる．「良い」関数のことを**特殊関数**と呼ぶことにしよう．パンルベは新しい特殊関数を，非線形微分方程式の解として見つけようと考えた．というのは，指数関数 e^x，三角関数 $\sin x, \cos x$，そして19世紀に盛んに研究された楕円関数（その代表としてワイエルシュトラスの $\wp$ 関数）などの特殊関数は，それぞれ

$$y' = y, \quad y'' + y = 0, \quad {y'}^2 = 4y^3 - g_2 y - g_3$$

といった線形あるいは1階の非線形微分方程式の解として特徴付けられるからである．パンルベは

$$y'' = F(x, y, y')$$

という形の微分方程式を考えた．ここで F は有理関数である．解には特殊関数になってほしいので，解はどこまでも解析接続できてほしいし，勝手なところに分岐点が現れるようなことは避けたい．彼はそのような要請をみたす微分方程式を，優れたアイデアと卓越した技量で絞り込むことに成功し，6つの方程式が得られた．それらは**パンルベ方程式**と呼ばれる．6つのうちで形の簡単なほうから2つほど挙げておこう．

$$y'' = 6y^2 + x, \qquad (\mathrm{P_I})$$

$$y'' = 2y^3 + xy + \alpha. \qquad (\mathrm{P_{II}})$$

パンルベ方程式はモノドロミー保存変形の研究において再発見され，重要な方程式であることは認識されたが，特殊関数として活躍することはなく長く忘れられた存在であった．1970年代になって統計物理のイジング模型の記述にパンルベ方程式が現れることが発見され，パンルベ方程式はようやく特殊関数としての活動を始める．その後のパンルベ方程式研究の隆盛についてはここでは触れないが，1つだけ，ガロア理論と関係する既約性について述べておこう．

パンルベ方程式は新しい特殊関数を手に入れたいということで発見されたのだから，当然それまでに知られていた関数では表されないこと（既約性）が期待された．しかし既約性を示すのは難しい問題で，長い間未解決であった．1980年代になって，西岡啓二・梅村浩両氏がパンルベ第1方程式 ($\mathrm{P_I}$)（パンルベI）の既約性の証明に成功した．梅村は古典拡大という概念を与え，既知の関数で表されるということを定式化した．考え方は一般リウビル拡大と同様である．体の拡大 $L/\mathbb{C}(x)$ に対して体の拡大の列 (K) で $K_0 = \mathbb{C}(x)$ で $L \subset K_m$ となるものがあって，各 K_i が K_{i-1} に K_{i-1} の元を係数とする線形常微分方程式の解，代数方程式の解を添加するか，あるいはアーベル関数（楕円関数の拡張）へ K_{i-1} の元を代入したものを添加することで得られるとき，$L/\mathbb{C}(x)$ を古典拡大という．このとき各拡大 K_i/K_{i-1} に対してガロア群は線形群か有限群かアーベル群となるので，古典拡大のガロア群はそれらを積み重ねたものになる．古典拡大の考えはパンルベ自身に由来するものだが，梅村はそれを群の作用と結びつけたのである．西岡はパンルベIが線形常微分方程式に帰着しないことを示し，梅村はその結果を利用してパンルベが古典拡大に含まれると矛盾が生じることを示した[3)]．

私が大学院生の頃，梅村さんがパンルベIの既約性について東大で集中講義をされた．その証明に成功したことは大きな話題であり，会場には多くの人が詰めかけて満員であった．梅村さんの講義はスマートで歯切れが良く，実に明快だった．驚いたことに，梅村さんがパンルベIの既約性の証明のアイデアを説明した翌日に，その講義を聴いていた野海さん[*1)]がパンルベII ($\mathrm{P_{II}}$) の既約性を証明してしまったのである．さらにその翌日（であったか)，岡本さん[*2)]がパンルベIVについても

*1)　野海正俊氏.
*2)　岡本和夫氏.

既約性の証明を与えた．「今この場所で（数学の）世界が動いたのだな」と強い印象を受けたことを覚えている．なお今ではすべてのパンルベ方程式の既約性が証明されている．

梅村らによるパンルベ方程式の既約性の証明は，既約でないとすると矛盾を生じるという論法であった．これに対して，非線形微分方程式に対してもガロア理論をきちんと構築して，ガロア群を求めることで既約性を示そうという研究も進められている．そのようなガロア理論は，梅村，マルグランジュ，ラミスといった人々により考案されている．先日京都であった研究集会では，ラミス氏が，パンルベ方程式についての非線形モノドロミー・非線形ストークス係数といった量を用いてガロア群を計算したい，という構想を話されていた．線形常微分方程式の場合と同様に，解の多価性が甚だしければガロア群が大きくなるという着想と考えられる．

5. ハミルトン系とガロア理論

天体力学をはじめ物理における様々な方程式は**ハミルトン系**の形で与えられる．ハミルトン系とは，時間変数 t に依存する $2n$ 個の未知関数 $q_1(t),\dots,q_n(t),p_1(t),\dots,p_n(t)$ についての連立1階常微分方程式

$$\frac{dq_i}{dt}=\frac{\partial H}{\partial p_i},\ \frac{dp_i}{dt}=-\frac{\partial H}{\partial q_i}\quad(1\le i\le n)\qquad \text{(H)}$$

のことである．ここで $H=H(t,q,p)$ はハミルトニアンと呼ばれる $t,q=(q_1,\dots,q_n)$, $p=(p_1,\dots,p_n)$ を変数とする関数である．ハミルトニアンが t に依存しない場合を自励系という．多くの場合ハミルトン系は自励系となるので，以下では自励系に限ることにする．さてその場合には，ハミルトニアン $H(q,p)$ にハミルトン系 (H) の解を代入すると定数となることがわかる（合成関数の微分法の簡単な演習問題）．一般に (t,q,p) の関数で解を代入すると定数となるものを**第1積分**という．すなわちハミルトン系においては，はじめから第1積分が1つ求まっているのである．

さて，ハミルトニアン H に加えて $n-1$ 個の第1積分 $F_2(q,p),\dots,F_n(q,p)$ で H も込めて関数的独立なものが存在したとしよう．$H(q,p)=F_1(q,p)$ とおく．さらに $F_1,\dots,F_n$ が互いにポアソン可換であるとする．ここで $F(q,p)$ と $G(q,p)$ がポアソン可換とは，

$$\{F,G\}:=\sum_{k=1}^{n}\left(\frac{\partial F}{\partial p_k}\frac{\partial G}{\partial q_k}-\frac{\partial F}{\partial q_k}\frac{\partial G}{\partial p_k}\right)=0$$

となることである．このとき，(q,p) から (x,y) への正準変換と呼ばれる変数変換 φ で，

$$F_i\circ\varphi(x,y)=y_i\quad(1\le i\le n)$$

となるものが存在する[4)]．ただし正準変換とは，ハミルトン系の形を保つような変換のことである．よって $K(x,y)=F_1\circ\varphi(x,y)$ が変換後のハミルトニアンとなり，ハミルトン系 (H) は

$$\frac{dx_i}{dt}=\frac{\partial K}{\partial y_i},\quad \frac{dy_i}{dt}=-\frac{\partial K}{\partial x_i}\quad(1\le i\le n)$$

へと変換される．ところが $K(x,y)=F_1\circ\varphi(x,y)=y_1$ となっているので，これの解は $x_1(t)$ が t の1次式で他の $x_i(t),y_i(t)$ は定数として求められてしまう．よってこの解を φ で戻すと，(H) の解 $q(t),p(t)$ が求められたことになる．このことから，ハミルトン系 (H) に対して独立で互いにポアソン可換な n 個の第1積分が存在する場合を**可積分**と呼ぶ．

ハミルトン系が可積分であるかを判定する，というのは基本的で重要な問題と考えられている．その判定に，ガロア理論（ピカール・ヴェシオ理論）を使うことができるという興味深い研究があるので紹介しよう．一般に $x_1(t),\dots,x_m(t)$ に対する連立1階常微分方程式

$$\frac{dx_i}{dt}=F_i(x_1,\dots,x_m)\quad(1\le i\le m)$$

に対して，$\phi(t)=(\phi_1(t),\dots,\phi_m(t))$ を1つの解とするとき，別の未知関数 $\xi_1(t),\dots,\xi_m(t)$ に対する「線形」常微分方程式

$$\frac{d\xi_i}{dt}=\sum_{j=1}^{m}\frac{\partial F_i}{\partial x_j}(\phi(t))\xi_j\quad(1\le i\le m)$$

を変分方程式という．変分方程式は，元の微分方

程式の解の初期値に関する微分可能性を示すときに用いられるものである．変分方程式は線形常微分方程式なので，そのガロア理論であるピカール・ヴェシオ理論が適用できる．物理の問題は普通実変数で考えるが，以下では独立変数 t も未知関数 q_i, p_i も複素数値とする．

さて，モラレスとラミスは，ハミルトン系の可積分性に関して次のような結果を示した[5]．ハミルトン系 (H) が可積分であるとする．そして n 個の第 1 積分は有理型関数となっていると仮定する．このとき (H) に対する変分方程式のガロア群の単位元の連結成分は可換となる．

線形常微分方程式がいくつかのパラメーターに依存するとき，そのガロア群が「小さく」なるようなパラメーターの値は一般にとびとびにしか現れないと思われる．よってモラレス・ラミスの定理を用いると，パラメーターを含むハミルトン系はほとんどのパラメーターの値について可積分とならない，という形の結果が得られるであろう．実際に発表直後から現在に至るまで，モラレス・ラミスの定理は様々なハミルトン系の非可積分性の証明に用いられてきている．

一方ガロア群が可換になるのは，微分方程式が高いレベルで可約になるということに対応している．ここ 10 年ほどの間に複素領域における線形常微分方程式の研究は著しく進み，特にリジッドな（すなわちアクセサリー・パラメーターを持たない）微分方程式については，既約であるための条件は完全に記述されている[6]．そのような結果と組み合わせることで，可積分なハミルトン系を系統的に求めるというようなことも可能なのかもしれない．

6. 結び

微分方程式のガロア理論について述べるとき，真っ先に挙げなければならない名前はソフォス・リーであった．リーは微分方程式に対してもガロア理論的な研究をしたいと考え，そのために必要な概念・基盤的な理論を整備していった．リー群・リー環の理論などそこで得られた成果はきわめて重要なもので，現在では微分ガロア理論を越えて代数・幾何・解析・物理学といったあらゆる領域に深く浸透している．本稿ではガロア理論的色彩が鮮明に見えるような微分方程式研究を取り上げることにしたため，リーの仕事はその普遍性ゆえにはずすことになってしまった．

第 2 節で述べたように，微分方程式研究の主流は解が求まらない中で何とかして解の挙動を調べるという解析学である．その中にあって微分方程式のガロア理論は，代数的な切り口で微分方程式のある一面を捉える理論と考えられる．代数的な見方はときに非常に有効で，微分方程式の美しい側面を鮮やかに浮かび上がらせる．一方で線形常微分方程式のガロア群がモノドロミー群のザリスキ閉包となることからもわかるように，ガロア理論には精密な情報を見ずに大まかに捉えるというところがあるように思われる．それはガロア理論の威力の源であると同時に，限界をも与える．例えば射影モノドロミーがフックス群となるような微分方程式は数論や代数幾何にとっても興味深い対象であるが，モノドロミー群のザリスキ閉包をとってしまうとその精妙な構造は見えなくなってしまう．そのような「性格」をよく把握した上でガロア理論に威力を発揮してもらうのが，微分方程式とガロア理論双方にとって幸せなことであろう．

参考文献

1) 久賀道郎,『ガロアの夢—群論と微分方程式』, 日本評論社, 1968.
2) J. Martinet and J.P. Ramis, Théorie de Galois différentielle et resommation, *Computer Algebra and Differential Equations*, 115–214, Academic Press, 1989.
3) 梅村浩, Painlevé 方程式の既約性について, 数学, **40** (1988), 47–61.
4) 伊藤秀一,『常微分方程式と解析力学』, 共立出版, 1998.
5) J.J. Morales-Ruiz and J.P. Ramis, Galoisian obstructions to integrability of Hamiltonian systems I, II, *Methods Appl. Anal.*, **8** (2001), 33–95, 97–111.
6) T. Oshima, Fractional calculus of Weyl algebra and Fuchsian differential equations, *MSJ Memoirs*, **28** (2012), 203pp.

（はらおか・よししげ，熊本大学大学院自然科学研究科）

可換代数と統計学

日比 孝之

1. 歴史的背景

可換代数は，歴史上，代数幾何，整数論，不変式論，表現論などとの相互関係を持ちながら発展してきた．たとえば，筆者の師匠の著[6)]の序文は，1970年代までの可換代数の潮流を概観している．しかしながら，従来，全く疎遠であった異分野との交流という観点から眺めるならば，1975年のRichard Stanleyの仕事[8)]を始祖とする，「可換代数と組合せ論」[3,4,9)]と呼ばれる境界分野の誕生は，特筆に値する．

可換代数と組合せ論の斬新な潮流は，その後，1980年代後半から台頭するグレブナー基底の数学[5)]とも馴染み，1990年代以降，単項式イデアル[2)]，二項式イデアル，凸多面体の三角形分割[10)]などの研究が爆発的に展開されている．

更に，1990年代後半に至り，グレブナー基底は統計学にも深い影響を及ぼし，「計算代数統計」と呼ばれる斬新な研究領域が誕生する[1,7)]．数学セミナー[12)]の特集「グレブナー基底の新天地」における，竹村彰通（東京大学）と青木敏（鹿児島大学）の紹介記事が詳しい．

本稿では，「可換代数は統計学にも使える！」ということを披露する．予備知識としては，多項式環のイデアルの定義を知っている程度で十分である．統計学の知識は不要である．

可換代数と統計学の相互関係を，二項式の可換代数の観点から探究し，境界分野「可換代数と統計学」の礎（いしずえ）を築くことは，現代の可換代数のもっとも斬新な潮流の一つである．

2. 統計的仮説検定

巷（ちまた）では，随分と統計学がもてはやされており，街の本屋さんの書棚には，おびただしい種類の統計学の本が，所狭しと並んでいる．

まず，本稿で扱う統計学の問題の一つを挙げよう．

或る特定の病気に罹患している患者100名のABO式血液型の遺伝子型を調べたところ，下記の表の結果を得た．その病気と血液型は何らかの関連があるか？

遺伝子型	AA	AB	AO	BB	BO	OO
人数	23	10	15	6	17	29

いま，その患者100名が持つ遺伝子（A遺伝子，B遺伝子，O遺伝子）の個数を調べる．単なる個数の計算であるが，敢えて，行列を使って下記のように記載する．そうすると，A遺伝子71個，B遺伝子39個，O遺伝子90個となる．

$$\begin{bmatrix} 2 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 2 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 2 \end{bmatrix} \begin{bmatrix} 23 \\ 10 \\ 15 \\ 6 \\ 17 \\ 29 \end{bmatrix} = \begin{bmatrix} 71 \\ 39 \\ 90 \end{bmatrix}.$$

無作為に選ばれた集団における，ABO式血液型の遺伝子型の出現確率は，その集団におけるA遺

伝子，B 遺伝子，O 遺伝子の個数に比例する（**ハーディ・ワインベルクの法則**）．すると，ハーディ・ワインベルクの法則を仮定することができる集団においては，遺伝子の個数 $[71, 39, 90]^\top$ から遺伝子型の統計的な推論を行うことができる．それゆえ，統計学の世界では，$[71, 39, 90]^\top$ を（ハーディ・ワインベルクの法則を仮定したときの）**十分統計量**と呼ぶ．

いま，この 100 人の集団における A 遺伝子，B 遺伝子，O 遺伝子の比率は，それぞれ，$\frac{71}{200}, \frac{39}{200}, \frac{90}{200}$ であるから，ハーディ・ワインベルクの法則に従う．ということは，AA, AB, AO, BB, BO, OO の遺伝子型の出現確率は，それぞれ，$(\frac{71}{200})^2, \frac{2\cdot71\cdot39}{200^2}, \ldots$ となる．

ここで，遺伝子型の期待値を表にすると

AA	AB	AO	BB	BO	OO
12.6025	13.845	31.95	3.8025	17.55	20.25

となる．

前ページの観測値（＝人数）の表と期待値の表を眺めると，随分と隔（へだ）たりがあるように思われるが，実際に隔たりがある（すなわち，この集団の患者が罹患する病気が，血液型の遺伝子型に何らかの影響を及ぼす疾患である）のか，それとも（実際は，この集団でもハーディ・ワインベルクの法則が成立しており，観測された隔たりは）偶然の結果と考えても不自然がないのか，を判定するのが**統計的仮説検定**である．その統計的仮説検定を遂行する常套手段の一つが**フィッシャーの正確確率検定**である．

■ 3. フィッシャーの正確確率検定 ■

連立線型方程式

$$\begin{bmatrix} 2 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 2 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 2 \end{bmatrix} \begin{bmatrix} x_{\mathrm{AA}} \\ x_{\mathrm{AB}} \\ x_{\mathrm{AO}} \\ x_{\mathrm{BB}} \\ x_{\mathrm{BO}} \\ x_{\mathrm{OO}} \end{bmatrix} = \begin{bmatrix} 71 \\ 39 \\ 90 \end{bmatrix}$$

の非負整数解

$$\boldsymbol{x} = [x_{\mathrm{AA}}, x_{\mathrm{AB}}, x_{\mathrm{AO}}, x_{\mathrm{BB}}, x_{\mathrm{BO}}, x_{\mathrm{OO}}]^\top$$

を考える．

これは何をやっているのか？と統計学の素人は疑問に思う．しかし，前ページの行列の計算をじっと眺めると，結局，100 人の集団があって，その 100 人が持つ 200 個の遺伝子が，A 遺伝子 71 個，B 遺伝子 39 個，O 遺伝子 90 個であるとき，その集団における出現可能な遺伝子型の重複集合（**事象**と呼ぶ）が，連立線型方程式の非負整数解である．

極端な話，AB 型 10 人，AO 型 61 人，BO 型 29 人の 100 人の集団でも，A 遺伝子 71 個，B 遺伝子 39 個，O 遺伝子 90 個となる．ところが，100 人を無作為に選んで，こんな極端な事象が偶発する可能性は，ハーディ・ワインベルクの法則を仮定するならば，ほとんど皆無であろう．逆に言うと，その集団が，或る「条件」を満たす 100 人を集めたものであるとすると，その「条件」は，血液型と何らかの関係があるのでは，と疑うことは自然であろう．

しかしながら，なんとなく偏っている雰囲気がある，と思われても，実際に偏っているのか，あるいは，偶然の偏りの範囲を越えないのか，を厳密に判定する必要がある．

フィッシャーの正確確率検定とは，冒頭の連立線型方程式の非負整数解，すなわち，出現の可能性のある事象を全列挙し，ハーディ・ワインベルクの法則に従うという仮説の下で，観測データ（前節冒頭の表）以上の珍しい事象が出現する確率（いわゆる p 値）を計算し，その観測データが，偶然の域を越えないのか否かを厳密に判定する手段である．

もう少し，詳しく説明する．冒頭の連立線型方程式の非負整数解 $\boldsymbol{x} = [x_{\mathrm{AA}}, \ldots, x_{\mathrm{OO}}]^\top$ があったとき，$\chi^2(\boldsymbol{x})$ を，前節の遺伝子型の期待値を使い，

$$\frac{(x_{\mathrm{AA}} - 12.6025)^2}{12.6025} + \cdots + \frac{(x_{\mathrm{OO}} - 20.25)^2}{20.25}$$

と定義する．すると，$\chi^2(\boldsymbol{x})$ が大きい事象は，期待値から離れていることになり，そのような事象は珍しいと言える．

いま，観測データを $\boldsymbol{x}^{(0)} = [23, \ldots, 29]^\top$ とするとき，

$$\chi^2(\boldsymbol{x}) \geq \chi^2(\boldsymbol{x}^{(0)})$$

となる事象 $\boldsymbol{x}$ が（ハーディ・ワインベルクの法則を仮定したときに）出現する確率を p 値（**有意確率**）と呼ぶ．その p 値を計算（する公式は省略するが，兎も角，計算）し，**有意水準**（たとえば，0.05）と比較し，p 値が 0.05 以下ならば，ハーディ・ワインベルクの法則に従うという**仮説を破棄**する．

計算機を使うと，冒頭の連立線型方程式の非負整数解の個数は 12240 個である．それほど多くはないから，p 値を計算することは可能である．実際，p 値は 0.00002387816 である．すると，0.05 よりも小さいから，仮説は棄却される．換言すると，前節冒頭の 100 人の集団が罹患している病気と遺伝子型は何らかの関係がある，と結論される．

■ 4. マルコフ連鎖モンテカルロ法 ■

しかしながら，一般には，連立線型方程式の非負整数解をすべて列挙することは，きわめて困難である．そうすると，フィッシャーの正確確率検定を遂行することは断念しなければならない．そこで登場するのが，**マルコフ連鎖モンテカルロ法**である．簡単に言うと，非負整数解をすべて列挙するのではなく，非負整数解の一部を抽出（サンプリング）し，それを使い，正確確率検定を実行するのである．

一般に，整数を成分とする d 行 n 列の行列 $A = (a_{ij})_{\substack{1 \leq i \leq d \\ 1 \leq j \leq n}}$ が**配置行列**であるとは，実数を成分とするベクトル $[r_1, \ldots, r_d]$ で，条件

$$\sum_{i=1}^{d} r_i a_{ij} = 1, \quad j = 1, \ldots, n \tag{1}$$

を満たすものが存在するときに言う．換言すると，行列 A が配置行列であるとは，原点を通過しない $\boldsymbol{R}^d$ の超平面 $\mathcal{H}$ で，A のすべての列ベクトルを含むものが存在することである．

前節の議論を踏襲し，本稿で扱う**統計モデル**とは，十分統計量 $[c_1, \ldots, c_d]^\top$ を持ち，配置行列を係数行列とする連立線型方程式

$$A \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} c_1 \\ \vdots \\ c_d \end{bmatrix} \tag{2}$$

で表現されるものとする．

なお，第 3 節の冒頭の連立線型方程式の係数行列は，3 変数二次の **Veronese 配置**と呼ばれ，配置行列である．実際，$[\frac{1}{2}, \frac{1}{2}, \frac{1}{2}]$ は，条件 (1) を満たすベクトルである．

係数行列が配置行列であるという仮定は，具体的な統計モデルでは，ほとんど満たされるから，不自然ではない．配置行列という仮定が必要である理由は，第 5 節で触れる．

以下，連立線型方程式 (2) の同次型

$$A \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix} \tag{3}$$

も扱う．

一般に，同次型 (3) の解 b と非同次型 (2) の解 $\boldsymbol{y}$ があったとき，$\boldsymbol{y} \pm b$ は，再び，非同次型 (2) の解となる．これは，線型代数でもお馴染みの簡単な事実である．その事実を踏まえ，マルコフ基底を導入する．

マルコフ基底とは，以下の条件（☆）を満たす，同次型の連立線型方程式 (3) の解となる整数ベクトル（非負でなくてもよい）の有限集合 $\mathcal{B} = \{ b^{(1)}, b^{(2)}, \ldots, b^{(s)} \}$ のことである．

（☆） 非同次型の連立線型方程式 (2) の非負整数解 $\boldsymbol{y}$ と $\boldsymbol{z}$ があったとき，整数 $q \geq 1$ と $b^{(i_1)}, \ldots, b^{(i_q)} \in \mathcal{B}$ と $\varepsilon_1, \ldots, \varepsilon_q \in \{ 1, -1 \}$ が存在し，次の (i) と (ii) を満たす．

(i) $\boldsymbol{z} = \boldsymbol{y} + \varepsilon_1 b^{(i_1)} + \varepsilon_2 b^{(i_2)} + \cdots + \varepsilon_q b^{(i_q)}$.

(ii) 任意の $1 \leq s \leq q$ について

$$\boldsymbol{y} + \sum_{k=1}^{s} \varepsilon_k b^{(i_k)}$$

は，非負整数ベクトルである．

換言すると，マルコフ基底とは，非同次型 (2) の任意の非負整数解 $\boldsymbol{y}$ から任意の非負整数解 $\boldsymbol{z}$

に，非負整数解を辿って到達する道筋（(☆) の (i) ならば，q 歩のステップ）を作る，同次型 (3) の有限個の整数解のことである．

マルコフ基底は存在する．マルコフ基底は係数行列に依存する概念であり，十分統計量とは無関係である．

マルコフ基底の「存在」と「計算」は後回しとし，マルコフ基底があったとき，正確確率検定をどのように実行するかを紹介する．

まず，非同次型 (2) の非負整数解として，観測データ

$$\boldsymbol{y}^{(0)} = [y_1^{(0)}, \ldots, y_n^{(0)}]^\top$$

を選ぶ．次に，マルコフ基底の元 b を無作為に，$\varepsilon \in \{1, -1\}$ を等確率で選ぶ．いま，$\boldsymbol{y}^{(0)} + \varepsilon b$ が負の成分を含めば，$\boldsymbol{y}^{(1)} = \boldsymbol{y}^{(0)}$ とし，$\boldsymbol{y}^{(0)} + \varepsilon b$ が非負整数ベクトルであれば，或る確率（詳細は省略）で，$\boldsymbol{y}^{(1)} = \boldsymbol{y}^{(0)}$ とするか，あるいは，$\boldsymbol{y}^{(1)} = \boldsymbol{y}^{(0)} + \varepsilon b$ とするかを決定する．以下，この操作を十分に多くの回数繰り返し，非同次型 (2) の非負整数解の列 $\boldsymbol{y}^{(0)}, \boldsymbol{y}^{(1)}, \ldots, \boldsymbol{y}^{(N)}$ が得られたならば，これらを非同次型 (2) の非負整数解の（妥当な）サンプル（とすることが可能であることが保証されているから，それらをサンプル）とし，p 値を推定する．これが，マルコフ連鎖モンテカルロ法である．

具体例を紹介する．或るホテルのレストランには，2 種類のケーキ（C ケーキと T ケーキ）が沢山ある．小テーブルが幾つかあり，それぞれの小テーブルには小皿 2 枚，中皿 2 枚，大皿 2 枚がある．一つの小テーブルに一人が座り，ケーキを 6 個選び，1 枚の皿に 1 個ずつ置く．下記の表は，79 人のケーキと皿の組合せである．なお，ケーキと皿の組合せは，全部で 27 通りであるが，0 人の組合せは表から省いてある．

小皿中皿大皿／小皿中皿大皿	人数
CCT／CCT	10
CCT／TTT	27
CCT／TCT	12
CCT／CCC	9
TTT／TTT	7
TTT／TCT	6
TTT／CCC	6
TCT／CCC	2

興味ある問題は，ケーキの種類と置く皿の種類に何らかの関連があるか，ということである．十分統計量は次の表となる．

小皿 C	小皿 T	中皿 C
85	73	105
中皿 T	大皿 C	大皿 T
53	17	141

更に，連立線型方程式は

$$A \begin{bmatrix} x_1 \\ \vdots \\ x_{27} \end{bmatrix} = \begin{bmatrix} 85 \\ 73 \\ 105 \\ 53 \\ 17 \\ 141 \end{bmatrix} \tag{4}$$

である．但し，配置行列 $A = (a_{ij})_{\substack{1 \le i \le 6 \\ 1 \le j \le 27}}$ のそれぞれの j 列は

$$a_{1j} + a_{2j} = a_{3j} + a_{4j} = a_{5j} + a_{6j} = 2$$

を満たす非負整数を成分とする．そのような列ベクトル 27 個を並べたものが A である．すなわち，

$$A = \begin{bmatrix} 2 & 2 & 2 & \cdots & 1 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 0 & \cdots & 1 & \cdots & 2 & 2 & 2 \\ 2 & 2 & 1 & \cdots & 1 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 1 & \cdots & 1 & \cdots & 2 & 2 & 2 \\ 2 & 1 & 2 & \cdots & 1 & \cdots & 2 & 1 & 0 \\ 0 & 1 & 0 & \cdots & 1 & \cdots & 0 & 1 & 2 \end{bmatrix}$$

となる．この配置行列は **Segre–Veronese 配置**と呼ばれるものである．

ケーキと皿の統計モデルのマルコフ連鎖モンテカルロ法による検定は，第 6 節を参照されたい．

5. トーリックイデアル

マルコフ基底の「存在」と「計算」を議論する．そのためには，舞台にイデアルを登壇させなければならない．

配置行列 $A=(a_{ij})_{\substack{1\le i\le d\\ 1\le j\le n}}$ があったとき，同次型の連立線型方程式 (3) の整数解

$$b=[b_1,\dots,b_n]^\top$$

に，変数 $x_1,\dots,x_n$ の**二項式**

$$f_b=\prod_{b_j>0}x_j^{b_j}-\prod_{b_j<0}x_j^{-b_j}$$

を対応させる．二項式とは，次数の等しい二つの単項式の差である．

なお，係数行列 A は配置行列であるから，条件 (1) を使えば，$b=[b_1,\dots,b_n]^\top$ が (3) の解であれば

$$b_1+\cdots+b_n=0$$

が従う．すると，$\prod_{b_j>0}x_j^{b_j}$ と $\prod_{b_j<0}x_j^{-b_j}$ の次数は等しい．

体 K 上の n 変数多項式環 $K[x_1,\dots,x_n]$ を準備する．体とは，加減乗除の演算が可能な代数系のことであるが，馴染みがなければ，多項式環とは，実数を係数とする変数 $x_1,\dots,x_n$ の多項式の全体を考えると思ってもよい．

配置行列 A の整数解 b に付随する二項式 f_b のすべてが生成する $K[x_1,\dots,x_n]$ のイデアルを I_A と表し，配置行列 A の**トーリックイデアル**と呼ぶ．多項式環の任意のイデアルは有限生成である（**Hilbert 基底定理**）から，(3) の有限個の整数解 $b^{(1)},b^{(2)},\dots,b^{(s)}$ が存在し，I_A は $f_{b^{(1)}},f_{b^{(2)}},\dots,f_{b^{(s)}}$ で生成される．

たとえば，第 3 節の 3 変数二次の Veronese 配置のトーリックイデアルの生成系は

$$x_1x_4-x_2^2,\quad x_1x_6-x_3^2,\quad x_4x_6-x_5^2,$$
$$x_2x_3-x_1x_5,\quad x_2x_5-x_3x_4,\quad x_3x_5-x_2x_6$$

である．

トーリックイデアルの生成系はマルコフ基底と対応する（Diaconis–Sturmfels）．換言すると，**同次型の連立線型方程式 (3) の整数解の有限集合 $\mathcal{B}=\{b^{(1)},b^{(2)},\dots,b^{(s)}\}$ がマルコフ基底であるためには，トーリックイデアル I_A が二項式 $f_{b^{(1)}},f_{b^{(2)}},\dots,f_{b^{(s)}}$ で生成されることが必要十分である．**

なお，『グレブナー道場』[5)]の定理 4.2.8 の証明を読む限り，この結果は，必ずしも，自明とは言えない．

トーリックイデアルの生成系を計算する一般論を紹介するには，グレブナー基底の知識が必要であるから，（冒頭で，「計算」を議論すると宣言しながら，何とも無責任ではあるが）本稿では割愛し，『グレブナー道場』[5)]の第 1 章に譲る．なお，具体的な配置行列があったとき，そのトーリックイデアルの生成系（とグレブナー基底）を計算するソフトと例題については，『グレブナー道場』[5)]の第 7 章を参照されたい．

6. Segre–Veronese 配置

第 4 節のケーキと皿の統計モデルをマルコフ連鎖モンテカルロ法で検定するには，(4) の係数行列のマルコフ基底を探す必要がある．

繰り返すが，連立線型方程式 (4) の係数行列は，Segre–Veronese 配置と呼ばれる配置行列である．煩雑であるから，Segre–Veronese 配置の定義は省くが，一般に，**Segre–Veronese 配置のトーリックイデアルの生成系は次数 2 の二項式からなる．**

すると，連立線型方程式 (4) の配置行列 A のトーリックイデアルの生成系は計算可能であるから，ケーキと皿の統計モデルのマルコフ基底が導ける．マルコフ基底の要素は，$\boldsymbol{R}^{27}$ の単位座標ベクトル $\boldsymbol{e}_1,\dots,\boldsymbol{e}_{27}$ を使うと，

$$\boldsymbol{e}_i+\boldsymbol{e}_j-\boldsymbol{e}_k-\boldsymbol{e}_l$$

なる表示を持つ，(4) の同次型

$$\begin{bmatrix} 2 & 2 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 2 & 2 \\ 2 & 2 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 2 & 2 \\ 2 & 1 & \cdots & 1 & 0 \\ 0 & 1 & \cdots & 1 & 2 \end{bmatrix} \begin{bmatrix} x_1 \\ \vdots \\ x_{27} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

の解から成る．但し，$i \neq j$, $\{i, j\} \cap \{k, \ell\} = \emptyset$ であるが，$k = \ell$ は許す．

ケーキと皿の統計モデルは，対立遺伝子の配列の問題を，わかりやすくするため，ケーキと皿で表現したものである．再び，ハーディ・ワインベルクの法則に従うという仮説を検証することになる．具体的に，一万個のサンプリングをし，p 値を推定すると，0.001644 となり，ハーディ・ワインベルクの法則に従うという仮説は破棄される．

以上，ケーキと皿の統計モデルの統計的仮説検定が，マルコフ連鎖モンテカルロ法で遂行できたことの背景には，その配置行列が Segre–Veronese 配置という，そのトーリックイデアルが可換代数で研究されており，生成系も既知であったという幸運（!?）が挙げられる．

■ 7. 回顧と展望 ■

可換代数の世界では，血液型の遺伝子モデルの Veronese 配置とともに，分割表[5, pp. 209–216)]の検定の配置行列（たとえば

$$\begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

など）を含む **Segre 配置**と呼ばれる配置は，古くから，研究対象であった．両者のトーリックイデアルは，次数 2 の二項式から成る生成系を持つことに着目し，その両者を一般化する概念とし，Segre–Veronese 配置が提唱され，そのトーリックイデアルも，次数 2 の二項式から成る生成系を持つことが示された．

記憶がいささか曖昧（あいまい）であるが，大杉英史（関西学院大学）と筆者が，竹村彰通と青木敏から，分割表のマルコフ基底の話を聞いたのは，2003 年であった．大杉英史と筆者は，1996 年以降，有限グラフに付随するトーリックイデアルの研究を継続しており，分割表の Segre 配置は，完全二部グラフに付随する配置であるから，われわれには，馴染み深い配置であった．

その後，2006 年の秋，京都大学数理解析研究所のプロジェクト研究「グレブナー基底の理論的有効性と実践的有効性」の公式行事の一つである研究集会が開催された折，統計モデルの配置行列のマルコフ基底が求まれば，マルコフ連鎖モンテカルロ法による統計的仮説検定が遂行できるから（代数から統計への逆転の着想であるが）トーリックイデアルの生成系が既知な配置行列に付随する統計モデルを（よしんば人工的であれ）創れば，（可換代数の研究者も）統計の論文がどんどん執筆できる，という話で盛り上がった．

そのとき，Segre–Veronese 配置がターゲットとなった．具体的な統計モデルとし，レストランで料理の注文をすることを考える．料理は，サラダ・スープ，メインディッシュ，ライス・パン，デザート，珈琲・紅茶の 5 品目から成る．注文の際は，サラダとスープのどちらかを，メインディッシュは魚料理と肉料理と野菜料理から二つを，ライスとパンのどちらかを，デザートは 5 種類のケーキから 3 種類を，珈琲と紅茶のどちらかを，それぞれ，選択する．すると，たとえば，100 人のお客さんが注文するデータがあったとき，そのデータから，メインディッシュの選択は，他の 4 品目の選択とは独立しているか否かを調べようとするならば，それは，Segre–Veronese 配置による統計的仮説検定のモデルとなる．従って，マルコフ連鎖モンテカルロ法による統計的仮説検定が遂行できる．

レストランでの料理の注文の統計モデルを一般化することから，groupwise selection problem と呼ばれる統計モデルが考案された．

他方，一つの統計モデルを創れば，それを更に複雑にした統計モデルを創ることはそんなに難しくはない．統計学は社会生活に密着している学問だからである．新しく創られた複雑な統計モデルを

可換代数の世界にフィードバックさせれば，トーリックイデアルの複雑かつ斬新な構成法の発想に繋がる．

複雑な一般 groupwise selection problem の具体例を挙げる．代数，幾何，統計の 3 科目の試験があり，それぞれの科目は 5 題から構成されている．受験者は，代数，幾何，統計の中から 2 科目を選択し，選択した科目の 5 題から 3 題を選び，合計 6 題を解答する．具体的なデータが与えられたとき，それぞれの問題は，「同じ科目内の他の問題の選択」あるいは「他の科目の選択」とは独立に，それぞれの問題の魅力によって選択されているかどうかを調査する．そのような統計モデルを解析する目的から Segre–Veronese 配置を一般化する，トーリックイデアルの「入れ子」と呼ばれるテクニックが提唱され，入れ子配置の理論が構築されている．

もはや紙面も尽きたが，JST CREST 日比プロジェクト「現代の産業社会とグレブナー基底の調和」[11)]（2008 年 10 月〜2014 年 3 月）では，可換代数から統計，統計から可換代数への流れを加速させ，計算代数統計を急激に発展させることに成功し，膨大な論文が出版されている．

本稿では，グレブナー基底の話題には触れなかった．マルコフ連鎖モンテカルロ法に必要なものは，あくまでも，トーリックイデアルの生成系だからである（グレブナー基底とは，際立った振る舞いをする生成系である）．しかしながら，トーリックイデアルがあったとき，その生成系のみに留まることなく，グレブナー基底を求めることは，理論と実践の両面から必須である．

ポスト日比プロジェクトとしては，竹村彰通が研究代表者，高山信毅（神戸大学）と筆者が研究分担者を務める，科研費基盤研究（S）「計算代数統計による統計と関連数学領域の革新」（平成 25〜29 年度）とともに，筆者が研究代表者を務める，科研費基盤研究（S）「統計と計算を戦略とする可換代数と凸多面体論の現代的潮流の誕生」（平成 26〜30 年度）が展開されている．両基盤研究（S）の研究活動の一環として，日本数学会季期研究所（MSJ SI）「グレブナー基底の 50 年」（2015 年 7 月，ホテル日航大阪）が開催される．更に，2016 年度には，京都大学数理解析研究所のプロジェクト研究「グレブナー基底の展望」も実施予定である．

参考文献

1) P. Diaconis and B. Sturmfels, Algebraic algorithms for sampling from conditional distributions, *Annals of Statistics* **26** (1998), 363–397.
2) J. Herzog and T. Hibi, “Monomial Ideals”, GTM 260, Springer, Berlin, 2011.
3) T. Hibi, “Algebraic Combinatorics on Convex Polytopes”, Carslaw, Glebe, N.S.W., Australia, 1992.
4) 日比孝之『可換代数と組合せ論』（シュプリンガー・ジャパン）1995 年（絶版）.
5) JST CREST 日比チーム（編）『グレブナー道場』（共立出版）2011 年.
6) 松村英之『可換環論』（共立出版）1980 年（復刊版，2000 年）.
7) G. Pistone and H.P. Wynn, Generalised confounding with Gröbner bases, *Biometrika* **83** (1996), 653–666.
8) R.P. Stanley, The upper bound conjecture and Cohen–Macaulay rings, *Stud. Appl. Math.* **54** (1975), 135–142.
9) R.P. Stanley, “Combinatorics and Commutative Algebra”, Second Ed., Progress in Math. 41, Birkhäuser, Boston, 1996.
10) B. Sturmfels, “Gröbner Bases and Convex Polytopes”, Amer. Math. Soc., Providence, RI, 1996.
11) 日比孝之，現代の産業社会とグレブナー基底の調和，数学 **65** (2013), 303–309.
12) 『数学セミナー』2012 年 2 月号.

（ひび・たかゆき，大阪大学大学院情報科学研究科）

計算機と代数

高山 信毅

1. 計算代数ソフトウェア

代数を扱うアルゴリズム，ソフトウェアはこの30年で長足の進歩をとげた．イデアル，ガロア群，ヒルベルト関数，自由分解，コホモロジー群等，筆者が代数学の講義を受講した頃には構成的なものとはほど遠いものであったが，グレブナー基底の理論，算法，実装により構成的で身近なものとなった．現在では多くの人がこれらの成果を活用している．一方，問題点としてはこれらの成果があまりに膨大となったため内部の仕組みが見えなくなっていることである．計算機ソフトウェアもその内面（どのような仕組みで計算しているのか）が見えないと，利用しているつもりが，逆に自分が振り回されることがよくある．坂村健先生の言[1]「人間は感性のみで勝負というのではなく，論理性をコンピューターに劣らないように磨きそれに人間なりの感性を加えないとコンピューターとの競争に負けてしまうであろう」を私なりに解釈すれば，計算機の内面（計算と論理）を知り人間なりの感性を加えていけば我々はもっと豊穣な世界を知ることができるであろう，となる．筆者は計算機の内面を知るにはプログラムを書いてみることが不可欠であると思っている．

2. 二項式に対する Buchberger アルゴリズム

計算機ソフトウェアの内面を知るために，ここでは一番の基礎であるグレブナー基底を計算する Buchberger アルゴリズムをなるべく短くプログラムとして実装してみよう．簡略にするため後述の二項式専用のものを作成する．グレブナー基底の理論は様々な本や記事で解説されているので，適宜これらを参照[2,3]しながら下記のプログラムを追っていただきたい．実装には最近話題の Sage（検索には sagemath）を用いる[*1]．

x^u と書いたら多重指数表現と解釈，つまり $x^u = \prod_{i=1}^n x_i^{u_i}$ と読んでほしい．二項式とは $x^u - x^v$ なる形の式である．Buchberger アルゴリズムを実装するには，n 次元のベクトル $u, v, \ldots$ に対して順序を指定，固定しないといけないが，これは n 次元（重み）ベクトル W を与えて，$u > v \Leftrightarrow u \cdot W > v \cdot W$ または（$u \cdot W = v \cdot W$ かつ $u - v$ の最初の 0 でない成分が正）と決める．二項式 f に対してこの順序で大きいほうの単項式を $\mathrm{in}_<(f)$（initial of f, f の先頭項）と書く．例えば $u > v$ なら $\mathrm{in}_<(x^u - x^v) = x^u$ である．二項式 f, g の大小比較は $\mathrm{in}_<(f)$ と $\mathrm{in}_<(g)$ で行う．プログラムを実装するには，まず二項式をどのような形でプログラム中に保持するか決めないといけない．ここでは $x^u - x^v$ を $u > v$ のときは `[1,u,v]`, $v > u$ のときは `[-1,v,u]` なるリストで保持するものとする．単項式 x^u は `[1,u,0]` なるリストで保持する．u, v の表現には Sage の vector 型データを用いる．n を変数 `NN` に保持する．

```
W=vector([1,1,1,1])
NN=len(W)
ff=[1,vector([1,0,0,1]),vector([0,1,1,0])]
def gtlex(F,G):
    for I in range(NN):
      if (F[1][I]>G[1][I]): return(1)
      if (F[1][I]<G[1][I]): return(-1)
    return(0)
def gt(F,G):
    if (G==0): return(1)
```

---

*1) 私は Sage については沼田泰英さんの “Sage の使用を視野に入れた Python 入門” を読んで 2 日でこの掲載プログラムを書いた初心者である．

```
    if (F==0): return(-1)
    Fw=F[1].dot_product(W)
    Gw=G[1].dot_product(W)
    if (Fw>Gw): return(1)
    if (Fw<Gw): return(-1)
    return(gtlex(F,G))
```

プログラム中の `ff` は二項式 $x_1x_4 - x_2x_3$ をどう表現するかの例である．`gt` は `F`, `G` が二項式のとき `F` > `G` なら 1，`F` < `G` なら -1，先頭項が定数倍を除き同じなら 0 を（値として）戻す．

次に実装すべきは単項式の割り算である．`pDivide(F,G)` は `F` が `G` で割り切れれば F/G を，割り切れないときは 0 を戻す．それから単項式 `F` と二項式 `G` のかけ算も実装の必要がある．これは `mmul(F,G)` で実現している．

```
def pDivide(F,G):
    if (F==0): return(0)
    M=zero_vector(NN)
    for I in range(NN):
        M[I]=F[1][I]-G[1][I]
        if (M[I] < 0): return(0)
    return([F[0]/G[0],M,0])
def mmul(F,G):
    if (F==0): return(0)
    return([F[0]*G[0],F[1]+G[1],F[1]+G[2]])
```

準備の最後は割り算による簡約化である（教科書によっては単に割り算と呼んでいる）．$p = \mathrm{in}_<(f)$ を $q = \mathrm{in}_<(g)$ が割り切るとき，f を $f-(p/q)g$ と書き換えるのが f の g による簡約である．簡約したものもまた二項式となることに注目してほしい．なおプログラムをなるべく短くするため簡約は後述の S-多項式の特別な場合であるという性質を利用している．

```
def pReduce(F,G):
    if (F==0): return(0)
    M=pDivide(F,G)
    if (M == 0): return(F)
    return(pReduce(spoly(F,G),G))
def pReduceBySet(F,Set):
    Changed=1
    while (Changed==1):
        Changed=0
        for I in range(len(Set)):
            if (pDivide(F,Set[I]) != 0):
                F=pReduce(F,Set[I]);
                if (F == 0): return(0)
                Changed=1; continue
    return(F)
```

`pReduce(F,G)` は二項式 `F` を二項式 `G` で簡約できなくなるまで何度も簡約する．`pReduceBySet(F,Set)` は二項式 `F` を二項式の集合 `Set` で簡約できなくなるまで簡約する．以上で準備完了である．与えられた二項式の集合 `L` からグレブナー基底を得るには `L` の二項式達の S-多項式を簡約し，その結果が 0 でなければ結果を `L` に加えていけばよい．どの二組の S-多項式を選んでも，簡約したものが 0 となればグレブナー基底を得られたこととなる．まず S-多項式を次の関数 `spoly(F,G)` で計算する．

```
def plcm(F,G):
    L=zero_vector(NN)
    for I in range(NN):
        if F[1][I]>G[1][I]: L[I]=F[1][I]
        else: L[I]=G[1][I]
    return([F[0],L,0])
def spoly(F,G):
    L=plcm(F,G);P=pDivide(L,F);Q=pDivide(L,G);
    N1=mmul(Q,[G[0],G[2],0]);
    N2=mmul(P,[F[0],F[2],0]);
    R=gt(N1,N2)
    if (R>0): return([N1[0],N1[1],N2[1]])
    if (R<0): return([-N2[0],N2[1],N1[1]])
    return(R)
```

最後に次の関数でグレブナー基底を求める．

```
def buchberger(L):
    N = len(L)
    Pairs=[]
    for I in range(N-1,-1,-1):
        for J in range(N-1,I,-1):
            Pairs=[[I,J]]+Pairs
    G=L
    while (len(Pairs) != 0):
        P = Pairs[0]
        Pairs = Pairs[1:]
        Sp = spoly(G[P[0]],G[P[1]])
        Rem = pReduceBySet(Sp,G)
        if (Rem != 0):
            G.append(Rem)
            for I in range(N):
                Pairs=[[I,N]]+Pairs
            N=N+1
    return(G)
```

なおこのプログラムは計算代数システム Risa/Asir で作成，テストしたものを Sage に移植したため Python でやると効率を落とす命令 `Pairs=Pairs[1:]` を使っている．これがよくないコードだと理解するには計算機の内面をメモリ管理のレベルで理解する必要がある．さて，例えば次のようにしてグレブナー基底を計算できる．

```
NN=6
W=vector([0,0,0,0,0,0])
Ell=[[1,vector([1,0,0,0,0,0]),vector([0,0,1,0,0,0])],
  [1,vector([1,1,0,0,0,0]),vector([0,0,0,1,0,0])],
  [1,vector([1,2,0,0,0,0]),vector([0,0,0,0,1,0])],
  [1,vector([1,3,0,0,0,0]),vector([0,0,0,0,0,1])]]
Gb=buchberger(Ell)
```

この例は $A = (a_{ij}) = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 \end{pmatrix}$ に対して $t_1^{a_{1j}} t_2^{a_{2j}} - x_j$, $j = 1, \ldots, 4$ のグレブナー基底を $\mathbf{Q}[t_1, t_2, x_1, x_2, x_3, x_4]$ で計算し，トーリックイデアル I_A の生成元（A のマルコフ基底）を計算する．なお基底は簡約されていなくて，余分な元をたくさん含む．余分な元を取り除き簡約グレブナー基底を求める関数を書くのはよい練習問題であろう．

3. 発展

上記のプログラムは Sage にそのまま入力すれば実行可能である．Buchberger アルゴリズムが 3 ページの記事で記述できることに驚く読者もいることを期待

している．このプログラムは短いものの，実装が正しいかどうかのテストが重要かつ難しく，元々の Risa/Asir のプログラムはテスト部分が本体の数倍ある．正しさを保証するには定義した関数のみたすべき性質を命題とし，それを証明するといった方法も有効である．さて，上記実装は効率的な計算は全くできていなくて，例えば二項式専門のシステムである `4ti2`[3, 7 章] を動かしてみるとそのスピードに感激すると思う．

Sage は軽量言語 Python を核として様々な数学ソフトウェアを統合して作成されたソフトウェアである．Sage を使うことにより代数学のどのような構成が計算機で可能か知ることもできる．Sage は直接ダウンロードしてもよいし，様々な数学ソフトウェアを編集収録したデスクトップ環境である MathLibre を取得すれば簡単に利用できる．様々な数学ソフトウェアを統合する試みは筆者らの始めた OpenXM プロジェクトや OpenMath プロジェクトが，最も古いと思われるが，現在最も成功したのはこの sagemath プロジェクトであろう．多くの人が参加できる，かつ，したくなる仕組みの構築には目を見張るものがある．

この文章を機会として，計算機の内面を知ることに興味を覚える人がいることを期待している．この例のように様々なアルゴリズムの原理を知るには短いプログラムを書けば十分であることも多い．様々な代数学の構成をプログラミングしてみることをお勧めしたい．いろんな言語やシステムを使ってみるのも楽しい．そんなときには `rosettacode.org` の例は大変参考になる．例えばこの記事のプログラムをいろいろな言語で実装してみるのもおもしろい．

コンピューターの内面を知ってほしくてこのような記事を書いたが，少しだけ研究の話題を．筆者自身は計算機による計算または理論的考察による代数的処理を前処理として数値解析をやるホロノミック勾配法とその統計への応用を研究中である[4]．その中で二項式のグレブナー基底も大活躍する．

なお，本文中に引用した文献，ソフトウェアで下記の文献表にないものは，検索によりインターネットより入手可能である．

参考文献

1) 毎日新聞 2014.11.20.
2) Cox, Little, O'Shea, *Ideals, Varieties, and Algorithms*, Springer (2006) (旧版には日本語訳もあり).
3) JST CREST 日比チーム（編），『グレブナー道場』，共立出版 (2011).
4) `http://www.math.kobe-u.ac.jp/OpenXM/Math/hgm`

（たかやま・のぶき，神戸大学大学院理学研究科）

微分方程式を考える

第7回

数学は現象をいかに記述しているか

ニュートンの運動方程式の初期値問題の大域解(2)

小澤 徹

平面運動を引き起こす力場の特徴付けについて考察し，平面の極座標表示を用いて，ニュートンの運動方程式の初期値問題の大域解の挙動を議論する．

7.1 平面運動を引き起こす力場

H を内積 $(\cdot|\cdot)$ を持つ実ヒルベルト空間とし, 連続な力の場 $F:\mathbb{R}_{\geq 0}\times H\times H\to H$ の下で，ニュートンの運動方程式に従う（単位質量を持つ）質点の運動を考える：

$$\begin{cases} x''(t)=F(t,x(t),x'(t)), \quad t\geq 0, \\ (x(0),x'(0))=(x_0,v_0). \end{cases} \tag{7.1}$$

ここに $(x_0,v_0)\in H\times H$ は初期時刻 $t=0$ において与えられた初期状態とする．この節では (7.1) の解 $x\in C^2([0,T^*);H)$ の一意的存在を仮定して議論を進める．ここに $0<T^*\leq\infty$ とする (解の存在と一意性に関する充分条件および T^* の特徴付けについては前回記述した)．さて, x_0 と v_0 の張る H の閉部分空間を $M=\mathrm{span}(x_0,v_0)$, 付随する H の直交分解を $H=M\oplus M^{\perp}$, H から M への直交射影を P とする．また, $t\in[0,T^*)$ に対し $M(t)=\mathrm{span}(x(t),x'(t))$ と置く．定義より $M(0)=M$ である．x_0 と v_0 が一次独立ならば $\dim M=2, x_0$ と v_0 が一次従属かつ $(x_0,v_0)\neq(0,0)$ ならば $\dim M=1$, $(x_0,v_0)=(0,0)$ ならば $\dim M=0$ となる．

定理 7.1 次は同値である．

(1) 任意の $t\in[0,T^*)$ に対し $M(t)\subset M$.

(2) 任意の $t\in[0,T^*)$ に対し $PF(t,x(t),x'(t))=F(t,x(t),x'((t))$.

(証明) **(1) $\Longrightarrow$ (2)**：方程式 (7.1) を区間 $[0,t]\subset[0,T^*)$ 上で積分し，両辺に有界作用素 P を作用させ，等式

$$x'(t)=v_0+\int_0^t PF(s,x(s),x'(s))ds$$

を得る．この両辺を微分すれば (2) が従う．

(2) $\Longrightarrow$ (1)：方程式 (7.1) を区間 $[0,t]\subset[0,T^*)$ 上で積分し，(2) を用いれば

$$x'(t)=P\left(v_0+\int_0^t F(s,x(s),x'(s))ds\right)\in M.$$

さらには

$$x(t)=x_0+\int_0^t x'(s)ds=P\left(x_0+\int_0^t x'(s)ds\right)\in M$$

を得るので (1) が従う．

定理 7.2 任意の $t\in[0,T^*)$ に対し，$M(t)=M$ であると仮定すると，各 t について $\alpha(t),\beta(t)\in\mathbb{R}$ が存在し，等式 $F(t,x(t),x'(t))=\alpha(t)x(t)+\beta(t)x'(t)$ が成立する．逆に，この等式が $[0,T^*)$ 上局所有界な関数 α,β により成立しているものとすると任意の $t\in[0,T^*)$ に対し $M(t)=M$ が成立する．

(証明) 任意の $t\in[0,T^*)$ に対し $M(t)=M$ ならば，定理 7.1 により $F(t,x(t),x'(t))\in M$ となるが，再び $M=M(t)$ を用いることで前半の主張が従う．後半の主張には $M\subset M(t)$ を示せば充分である．そこで $t_0\in[0,T^*)$ を任意に取り固定する．また $u\in M(t_0)^\perp$ を任意に取り $\varphi(t)=(x(t)|u),t\in[0,t_0]$ と置く．このとき $(x(t_0)|u)=(x'(t_0)|u)=0$ より

$$\varphi'(t)=-\int_t^{t_0}(\alpha(\tau)\varphi(\tau)+\beta(\tau)\varphi'(\tau))d\tau,$$
$$\varphi(t)=-\int_t^{t_0}\varphi'(s)ds$$

を得る．さて，$\psi(t)=|\varphi(t)|+|\varphi'(t)|$, $\gamma(t)=\max(|\alpha(t)|,|\beta(t)|+1)$ と置くと上の 2 つの等式より，不等式

$$\psi(t)\le\int_t^{t_0}\gamma(s)\psi(s)ds,\quad t\in[0,t_0]$$

を得る．右辺を $\Psi(t)$ と置くと $\psi(t)\le\Psi(t)$,

$$\Psi'(t)=-\gamma(t)\psi(t)\ge-\gamma(t)\Psi(t)$$

より

$$\frac{d}{dt}\left(\exp\left(-\int_t^{t_0}\gamma(s)ds\right)\Psi(t)\right)=\exp\left(-\int_t^{t_0}\gamma(s)ds\right)(\Psi'(t)+\gamma(t)\Psi(t))$$
$$\ge 0$$

が従うので

$$\exp\left(-\int_t^{t_0}\gamma(s)ds\right)\Psi(t)\le\exp\left(-\int_{t_0}^{t_0}\gamma(s)ds\right)\Psi(t_0)=0,$$

即ち，任意の $t\in[0,t_0]$ に対し $\varphi(t)=\varphi'(t)=0$ を得る．これより直ちに $x_0,v_0\in M(t_0)^{\perp\perp}=\overline{M(t_0)}=M(t_0)$ が従う．これが示すべきことであった．

定理 7.2 に現れる α,β は，一般に x,x' を通じて

$$\alpha(t)=f(t,x(t),x'(t)),\quad \beta(t)=g(t,x(t),x'(t))$$

なる形で表されるものであるから，平面運動を引き起こす力場 F は実数値関数 $f,g:\mathbb{R}_{\ge0}\times H\times H\to\mathbb{R}$ によって

$$F(t,x,v)=f(t,x,v)x+g(t,x,v)v \tag{7.2}$$

と表されるものと特徴付けられる．中心力場は $g\equiv0$ で f が実一変数関数 $\Phi:\mathbb{R}\to\mathbb{R}$ によって $f(t,x,v)=\Phi(\|x\|)$ と表される場合に相当し，平面運動を引き起こす力場として角運動量保存則の枠組みで説明されることが多い．一方，定理 7.1 および 7.2 は，角運動量や「空間の向き」の概念とは無関係に理解されるものである．

7.2 平面への座標の導入

さて，$\dim M\le 2$ であるので，3 つの場合について M に座標を導入することで (7.2) の形を持つ (7.1) の解の軌道を議論しよう．

[$\dim M=0$ **の場合**]

この場合は $x_0=v_0=0$ であるので，解の一意性により恒等的に $(x(t),x'(t))=(0,0)$ となる．

[$\dim M=1$ **の場合**]

この場合は $M=\mathrm{span}(x_0)$ または $M=\mathrm{span}(v_0)$ となる．$x_0\ne0$ の場合 $M=\mathrm{span}(x_0)$，$x_0=0$ の場合 $M=\mathrm{span}(v_0), v_0\ne0$ として考える．

(1) $M=\mathrm{span}(x_0), x_0\ne0$ **の場合**：$x(t)\in M=\mathrm{span}(x_0)$ であるから $x(t)=((x(t)|x_0)/\|x_0\|^2)x_0$ と表される．このとき $y(t)=(x(t)|x_0)/\|x_0\|$ と置くと $y\in C^2([0,T^*);\mathbb{R})$ であり，y は

$$\begin{cases} y''(t)=\alpha(t)y(t)+\beta(t)y'(t), \\ y(0)=\|x_0\|,\quad y'(0)=\dfrac{(v_0|x_0)}{\|x_0\|} \end{cases} \tag{7.3}$$

の解となっている．ここに

$$\alpha(t)=f\left(t,y(t)\frac{x_0}{\|x_0\|},y'(t)\frac{x_0}{\|x_0\|}\right),\quad \beta(t)=g\left(t,y(t)\frac{x_0}{\|x_0\|},y'(t)\frac{x_0}{\|x_0\|}\right)$$

である．

(2) $M=\mathrm{span}(v_0), v_0\ne0$ **の場合**：$x(t)\in M=\mathrm{span}(v_0)$ であるから

$x(t) = ((x(t)|v_0)/\|v_0\|^2)v_0$ と表される．このとき $y(t) = (x(t)|x_0)/\|v_0\|$ と置くと $y \in C^2([0,T^*);\mathbb{R})$ であり，y は

$$\begin{cases} y''(t) = \alpha(t)y(t) + \beta(t)y'(t), \\ y(0) = \dfrac{(x_0|v_0)}{\|v_0\|}, \quad y'(0) = \|v_0\| \end{cases} \tag{7.4}$$

の解となっている．ここに

$$\alpha(t) = f\left(t, y(t)\frac{v_0}{\|v_0\|}, y'(t)\frac{v_0}{\|v_0\|}\right), \quad \beta(t) = g\left(t, y(t)\frac{v_0}{\|v_0\|}, y'(t)\frac{v_0}{\|v_0\|}\right)$$

である．

[$\dim M = 2$ の場合]

この場合 x_0 と v_0 は一次独立であり，特に $\|x_0\| \neq 0$, $\|v_0\| \neq 0$, $0 \leq |(x_0|v_0)| < \|x_0\|\|v_0\|$ となっている．$e_1, e_2 \in \mathbb{R}^2$ を $|e_1| = |e_2| = 1$, $e_1 \cdot e_2 = 0$ なるものとする．ここに $u = (u_1, u_2)$, $v = (v_1, v_2) \in \mathbb{R}^2$ に対し $u \cdot v = u_1v_1 + u_2v_2$, $|u| = \sqrt{u \cdot u}$ であるとする．さて

$$T_\pm\left(\frac{x_0}{\|x_0\|}\right) = e_1, \quad T_\pm\left(\frac{v_0}{\|v_0\|}\right) = \frac{(x_0|v_0)}{\|x_0\|\|v_0\|}e_1 \pm \left(1 - \left(\frac{(x_0|v_0)}{\|x_0\|\|v_0\|}\right)^2\right)^{1/2} e_2$$

と定めると $M = \mathrm{span}(x_0, v_0) = \{\lambda x_0 + \mu v_0 \in H; \lambda, \mu \in \mathbb{R}\}$ 上で

$$T_\pm(\lambda x_0 + \mu v_0) = \left(\lambda\|x_0\| + \mu\frac{(x_0|v_0)}{\|x_0\|}\right)e_1 \pm \mu\left(1 - \left(\frac{(x_0|v_0)}{\|x_0\|\|v_0\|}\right)^2\right)^{1/2}\|v_0\|e_2$$

なる線形写像 $T_\pm : M \to \mathbb{R}^2$ が定まる．$T_\pm$ の値域 Range $T_\pm = \mathrm{span}(e_1, e_2) = \mathbb{R}^2$ より $T_\pm$ は全射である．また，等式

$$\begin{aligned} |T_\pm(\lambda x_0 + \mu v_0)|^2 &= \left(\lambda\|x_0\| + \mu\frac{(x_0 v_0)}{\|x_0\|}\right)^2 + \mu^2\left(1 - \left(\frac{(x_0 v_0)}{\|x_0\|\|v_0\|}\right)^2\right)\|v_0\|^2 \\ &= \lambda^2\|x_0\|^2 + 2\lambda\mu(x_0|v_0) + \mu^2\|v_0\|^2 \\ &= \|\lambda x_0 + \mu v_0\|^2 \end{aligned}$$

より $T_\pm$ は等距離，特に単射である．従って $T_\pm$ は M と $\mathbb{R}^2$ との線形同型を与える．さて $y(t) = T_\pm x(t)$ と置くと $y \in C^2([0,\infty);\mathbb{R}^2)$ であり y は

$$\begin{cases} y''(t) = T_\pm x''(t) = \alpha(t)y(t) + \beta(t)y'(t), \\ y(0) = T_\pm x_0 = \|x_0\|e_1, \\ y'(0) = T_\pm v_0 = \dfrac{(x_0|v_0)}{\|x_0\|}e_1 \pm \left(1 - \left(\dfrac{(x_0 v_0)}{\|x_0\|\|v_0\|}\right)^2\right)^{1/2}\|v_0\|e_2 \end{cases} \tag{7.5}$$

の解となっている．ここに

$$\alpha(t) = f(t, T_\pm^{-1}y(t), T_\pm^{-1}y'(t)), \quad \beta(t) = g(t, T_\pm^{-1}y(t), T_\pm^{-1}y'(t))$$

である．さて $y(t) \in \mathbb{R}^2$ を極座標表示し

$$y(t) = (r(t)\cos\theta(t), r(t)\sin\theta(t)) = r(t)e_\rho(t),$$
$$e_\rho(t) = (\cos\theta(t), \sin\theta(t))$$

と置く．$e_\rho(t)$ に垂直な単位ベクトルとして

$$e_\varphi(t) = (-\sin\theta(t), \cos\theta(t))$$

を取る．$e'_\rho(t) = \theta'(t)e_\varphi(t)$ および $e'_\varphi(t) = -\theta'(t)e_\rho(t)$ により

$$y'(t) = r'(t)e_\rho(t) + r(t)\theta'(t)e_\varphi(t),$$
$$y''(t) = (r''(t) - r(t)(\theta'(t))^2)e_\rho(t) + (2r'(\theta)\theta'(t) + r(t)\theta''(t))e_\varphi(t)$$

となるので (7.5) は

$$\begin{cases} r''(t) - r(t)(\theta'(t))^2 = \alpha(t)r(t) + \beta(t)r'(t), \\ 2r'(\theta)\theta'(t) + r(t)\theta''(t) = \beta(t)r(t)\theta'(t) \end{cases} \tag{7.6}$$

と同値となる．ここに

$$\alpha(t) = f(t, r(t)T_\pm^{-1}e_\rho(t), r'(t)T_\pm^{-1}e_\rho(t) + r(t)\theta'(t)T_\pm^{-1}e_\varphi(t)),$$
$$\beta(t) = g(t, r(t)T_\pm^{-1}e_\rho(t), r'(t)T_\pm^{-1}e_\rho(t) + r(t)\theta'(t)T_\pm^{-1}e_\varphi(t))$$

である．さて $e_1 = e_\rho(0), e_2 = e_\varphi(0)$ と定めると

$$r(0) = \|x_0\|, \quad r'(0) = \frac{(x_0|v_0)}{\|x_0\|}, \quad \theta'(0) = \pm\left(1 - \left(\frac{(x_0|v_0)}{\|x_0\|\|v_0\|}\right)^2\right)^{1/2}\frac{\|v_0\|}{\|x_0\|}$$

となる．特に

$$r(0) > 0, \quad \theta'(0) \neq 0$$

であり $l = r(0)^2\theta'(0)$ と置くと $l \neq 0$ となる．(7.6) の第 2 式は

$$\frac{d}{dt}(r(t)^2\theta'(t)) = \beta(t)r(t)^2\theta'(t)$$

と同値となる．

7.3 中心力場の場合

この節では，前節の議論を中心力場の場合に限定して考える．即ち，(7.1) の右辺が $\Phi : \mathbb{R} \to \mathbb{R}$ によって $F(t,x,v) = \Phi(\|x\|)x$ で与えられる場合を議論する．ポテンシャル関数 V を

$$V(r) = \int_0^r \Phi(\rho)\rho d\rho, \quad r \geq 0$$

で定めると，等式

$$(V \circ \|x\|)'(t) = V'(\|x(t)\|)\frac{d}{dt}\|x(t)\|$$

$$
\begin{aligned}
&= -\Phi(\|x(t)\|)\|x(t)\|\frac{d}{dt}\|x(t)\| = -\Phi(\|x(t)\|)\frac{1}{2}\frac{d}{dt}\|x(t)\|^2 \\
&= -\Phi(\|x(t)\|)(x(t)|x'(t)) = -(\Phi(\|x(t)\|)x(t)|x'(t)) \\
&= -(x''(t)|x'(t)) = -\frac{1}{2}\frac{d}{dt}\|x'(t)\|^2
\end{aligned}
$$

が成立するので，$E(t) = \frac{1}{2}\|x'(t)\|^2 + V(\|x(t)\|)$ で定義されるエネルギーは保存量となる．即ち，任意の $t \in [0, T^*)$ に対し，等式 $E(t) = E(0)$ が成立する．

[$\dim M = 1$ の場合]

(1) $M = \mathrm{span}(x_0)$, $x_0 \neq 0$ **の場合**：$y(t) = (x(t)|x_0)/\|x_0\|$ と置くと $y \in C^2([0, T^*); \mathbb{R})$ であり，y は

$$
\begin{cases} y''(t) = \Phi(|y(t)|)y(t), \\ y(0) = \|x_0\|, \quad y'(0) = \dfrac{(v_0|x_0)}{\|x_0\|} \end{cases} \tag{7.7}
$$

の解となっている．方程式 (7.7) に対する保存量は $\frac{1}{2}(y'(t))^2 + V(y(t))$ であり，$E(t)$ と一致するものである．

(2) $M = \mathrm{span}(v_0)$, $v_0 \neq 0$ **の場合**：$y(t) = (x(t)|v_0)/\|v_0\|$ と置くと $y \in C^2([0, T^*); \mathbb{R})$ であり，y は

$$
\begin{cases} y''(t) = \Phi(|y(t)|)y(t), \\ y(0) = \dfrac{(x_0|v_0)}{\|v_0\|}, \quad y'(0) = \|v_0\| \end{cases} \tag{7.8}
$$

の解となっている．方程式 (7.8) に対する保存量は (7.7) のものと同一である．

[$\dim M = 2$ の場合]

前節と同じ記号を用いて $y(t) = T_\pm x(t)$ と置くと $y \in C^2([0, T^*); \mathbb{R}^2)$ であり，y は

$$
\begin{cases} y''(t) = \Phi(|y(t)|)y(t), \\ y(0) = \|x_0\|e_1,\ y'(0) = \dfrac{(x_0|v_0)}{\|x_0\|}e_1 \pm \left(1 - \left(\dfrac{(x_0|v_0)}{\|x_0\|\|v_0\|}\right)^2\right)^{1/2} e_2 \end{cases} \tag{7.9}
$$

の解となっている．極座標表示 $y(t) = r(t)e_\rho(t)$ を用いると (7.9) の第 1 式は

$$
\begin{cases} r''(t) - r(t)(\theta'(t))^2 = \Phi(r(t))r(t), \\ (r^2\theta')'(t) = 0 \end{cases} \tag{7.10}
$$

と同値となる．$l = r(0)^2\theta'(0)$ と置くと $l \neq 0$ となり，任意の $t \in [0, T^*)$ に対し，等式 $r(t)^2\theta'(t) = l$ が成立する．特に，任意の $t \in [0, T^*)$ に対し $r(t) \neq 0, \theta'(t) \neq 0$ であることが分かる．以上より (7.10) の第 1 式は

$$
r''(t) - \frac{l^2}{r(t)^3} = \Phi(r(t))r(t) \tag{7.11}
$$

と書き換えられ, (7.11) に対する保存量は $E_{\mathrm{eff}}(t) = \frac{1}{2}(r'(t))^2 + \frac{l^2}{2(r(t))^2} + V(r(t))$ で定義される有効エネルギーとなる．

7.4 非集中型自己相互作用場の下での古典軌道 (1)

この節では $\Phi(r) = -r^{p-1}, 1 \le p < \infty$ で与えられる中心力場を考え，初期値問題

$$\begin{cases} x''(t) = -\|x(t)\|^{p-1}x(t), \quad t > 0, \\ (x(0), x'(0)) = (x_0, v_0) \end{cases} \tag{E^p_-}$$

について議論する．前回取り上げた問題とは，右辺の符号が逆となっている所が異なっている．$p = 1$ の場合，解は $x(t) = (\cos t)x_0 + (\sin t)v_0$ と具体的表示を持つので，以下では $p > 1$ の場合を考える．前回の定理 6.1 により $x \in C^2([0, T^*); H)$ なる解の存在と一意性が従い

$$E(t) = \frac{1}{2}\|x'(t)\|^2 + \frac{1}{p+1}\|x(t)\|^{p+1}$$

で定義されるエネルギーは保存量

$$E(t) = E(0), \quad t \in [0, T^*)$$

となる．これより

$$\sup_{t\in[0,T^*)} \|x'(t)\| \le (2E(0))^{\frac{1}{2}}, \qquad \sup_{t\in[0,T^*)} \|x(t)\| \le ((p+1)E(0))^{\frac{1}{p+1}} \tag{7.12}$$

が得られるので $T^* = \infty$，即ち x は大域解であり x は

$$x, x', x'' \in (C \cap L^\infty)([0, \infty); H)$$

なるクラスに属していることが分かる．特に (7.12) と (E^p_-) により，評価

$$\sup_{t\ge 0}\|x(t)\| \le ((p+1)E(0))^{\frac{1}{p+1}}, \tag{7.13}$$

$$\sup_{t\ge 0}\|x'(t)\| \le (2E(0))^{\frac{1}{2}}, \tag{7.14}$$

$$\sup_{t\ge 0}\|x''(t)\| \le ((p+1)E(0))^{\frac{p}{p+1}} \tag{7.15}$$

が成立し，古典軌道は有界に留まっていることが分かる．

そこで古典軌道を詳しく調べてみよう．まず (E^p_-) は円運動する解を持つことを示そう．その特徴付けは次で与えられる．

定理 7.3　(E^p_-) の解 $x \in C^2([0, \infty); H)$ に対し次は同値である：

(1)　任意の $t \ge 0$ に対し $\|x(t)\| = \|x_0\|$.

(2)　任意の $t \ge 0$ に対し $(x'(t)|x(t)) = 0$.

(3)　$x_0, v_0 \in H$ は $(v_0|x_0) = 0, \|x_0\|^{p+1} = \|v_0\|^2$ を満たし $x_0 \ne 0$ なるとき x は

$$x(t) = \cos(\|x_0\|^{\frac{p-1}{2}}t)x_0 + \frac{\sin(\|x_0\|^{\frac{p-1}{2}}t)}{\|x_0\|^{\frac{p-1}{2}}}v_0$$

と表される．

さらに，上の同値な命題が成り立つとき任意の $t \geq 0$ に対し等式

$$\|x(t)\|^{p+1} = \|x'(t)\|^2 = \|x_0\|^{p+1} = \|v_0\|^2 = \frac{2(p+1)}{p+3}E(0)$$

が成立する．

（証明） **(1) $\Longrightarrow$ (2)**：(1) の下で $(x'(t)|x(t))$ を計算すると

$$(x'(t)|x(t)) = \frac{1}{2}\frac{d}{dt}\|x(t)\|^2 = 0.$$

(2) $\Longrightarrow$ (1)：(2) の下で $\|x(t)\|^2$ を計算すると

$$\begin{aligned}\|x(t)\|^2 &= \|x(0)\|^2 + \int_0^t \frac{d}{ds}\|x(s)\|^2 ds \\ &= \|x_0\|^2 + 2\int_0^t (x'(s)|x(s))ds = \|x_0\|^2.\end{aligned}$$

よって，$\|x(t)\| = \|x_0\|$ となる．

(1) $\Longrightarrow$ (3)：まず $x_0 \neq 0$ の場合を考える．

$$x''(t) = -\|x_0\|^{p-1}x(t)$$

となるので直ちに解の表示を得る．(1) と同値な (2) において $t=0$ と置くと $(v_0|x_0) = 0$ が従う．解の表示を微分して

$$x'(t) = -\|x_0\|^{\frac{p-1}{2}}\sin(\|x_0\|^{\frac{p-1}{2}}t)x_0 + \cos(\|x_0\|^{\frac{p-1}{2}}t)v_0$$

を得るので $(v_0|x_0) = 0$ を用いると

$$(x'(t)|x(t)) = \frac{\sin(\|x_0\|^{\frac{p-1}{2}}t)\cos(\|x_0\|^{\frac{p-1}{2}}t)}{\|x_0\|^{\frac{p-1}{2}}}(\|v_0\|^2 - \|x_0\|^{p+1})$$

を得る．仮定 $\|x_0\| \neq 0$ と (2) より等式 $\|v_0\|^2 = \|x_0\|^{p+1}$ が従う．

次に $x_0 = 0$ の場合を考える．(1) より任意の $t \geq 0$ に対し $x(t) = 0$ となる．よって $t > 0$ に対して $x'(t) = 0$ となり $t \to 0$ として $v_0 = x'(0) = 0$ を得る．これより (3) が従う．

(3) $\Longrightarrow$ (2)：(1) $\Longrightarrow$ (3) と同様な計算による．

紙数が尽きたので，(E_-^p) の周期解など続きの話題は次回に述べる．

参考文献

1) 大谷光春，『理工基礎　常微分方程式論』，サイエンス社．
2) ゴールドスタイン，『古典力学』，吉岡書店．

（おざわ・とおる，早稲田大学理工学術院）

例題形式で探求する代数学のエッセンス

方程式から代数学の本質に迫る

第3回

2つの剰余定理

小 林　正 典

3.1 第3回の問題

今回は複数の点における条件を満たす多項式を求める問題を考えてみよう．

> **例題 3.1**　$f(x)$ を3次以下の実数係数多項式とする．
> $f(0)=-2,\ f(1)=-2,\ f'(1)=0,\ f(2)=4$ を満たすとき $f(x)$ を求めよ．

3.2 連立1次方程式による解法

微分が入っているので解析の問題にも見えるかもしれない．解析は苦手，と逃げられては困るので，まずは微分が入らない類題を素朴に解いてみよう．

> **問題 3.1**　$f(x)$ を3次以下の実数係数多項式とする．
> $f(0)=2,\ f(1)=2,\ f(2)=-2,\ f(3)=8$ を満たすとき $f(x)$ を求めよ．

解答　$f(x)=a+bx+cx^2+dx^3$ (a,b,c,d は実数) とおく．条件より $a=2$, $a+b+c+d=2$ などが従うが，行列を用いて次のように表せる．

$$\begin{pmatrix}1&0&0&0\\1&1&1&1\\1&2&4&8\\1&3&9&27\end{pmatrix}\begin{pmatrix}a\\b\\c\\d\end{pmatrix}=\begin{pmatrix}2\\2\\-2\\8\end{pmatrix}.$$

この連立1次方程式を掃き出し法を用いて解けばよい．係数行列の右に定数項をならべた「拡大係数行列」に対し，行基本変形を施して階段行列にする (詳細は線形代数のテキストを参照のこと)．

$$\left(\begin{array}{cccc|c} 1 & 0 & 0 & 0 & 2 \\ 1 & 1 & 1 & 1 & 2 \\ 1 & 2 & 4 & 8 & -2 \\ 1 & 3 & 9 & 27 & 8 \end{array}\right) \to \cdots \to \left(\begin{array}{cccc|c} 1 & 0 & 0 & 0 & 2 \\ 0 & 1 & 0 & 0 & 8 \\ 0 & 0 & 1 & 0 & -11 \\ 0 & 0 & 0 & 1 & 3 \end{array}\right).$$

よって $f(x) = 2 + 8x - 11x^2 + 3x^3$. □

注意 3.1 係数行列の行列式はヴァンデルモンド（Vandermonde）の行列式と呼ばれている．

例題 3.1 も，$f'(1) = 0$ という条件は $b + 2c + 3d = 0$ という 1 次方程式に過ぎないから，同様に解ける．実際に解くのは読者にお任せしたい（計算は大変ではない．答えは後述）．ところで，この種の条件が与えられたとき，解が常に一意的に存在するか，気にならないだろうか．

3.3 剰余定理による言い換え

剰余定理と同様にして，次が示せる．

定理 3.1（一般化された剰余定理） α を実数，m を正整数とする．実数係数多項式 $f(x)$ を $(x-\alpha)^m$ で割った余りは $\sum_{i=0}^{m-1} \frac{f^{(i)}(\alpha)}{i!}(x-\alpha)^i$ で与えられる[注1]．

注1 係数は標数 0 の体ならよい．微分は形式的に $(x^n)' = nx^{n-1}$ で与える．

これによると「$f(1) = -2,\ f'(1) = 0$」とは「$f(x)$ を $(x-1)^2$ で割った余りが -2」ということである．したがって例題は次のように言い換えられる．

例題 3.1 の言い換え 高々 3 次の多項式 $f(x)$ を x, $(x-1)^2$, $x-2$ で割った余りがそれぞれ $-2, -2, 4$ であるとき，$f(x)$ を求めよ．

これなら整数論に古典的な類似問題がある．江戸時代のベストセラー『塵劫記』[1)]に「百五減」という次のような数当て問題が載っている[注2]．

注2 表現は変えてある．

問題 3.2（百五減） ある自然数は，7 で割った余りが 2，5 で割った余りが 1，3 で割った余りが 2 であるという．105 未満であるとして，その数を求めよ．

解答（塵劫記の答） それぞれの余りに順に 15, 21, 70 を掛けて足し合わせ，出た結果が 105 以上となるときは 105 を何回か引いて，余りを求める．$2 \times 15 + 1 \times 21 + 2 \times 70 = 191$ となり，$191 - 105 = 86$ が答えである． □

注意 3.2 この 15, 21, 70 というのが何かというと，例えば 15 は 3 と 5 で割り切れて 7 で割った余りが 1 となる．したがって，整数 a, b, c に対し，$15a + 21b + 70c$ を 7, 5, 3 で割った余りはそれぞれちょうど a, b, c となるのである．

上の注意より，余りの組をどう指定しても条件を満たす自然数が存在する．果たして余りだけから元の数は一意的に決まるのだろうか？ 他の整数の組でも同じようにできるのであろうか？ 多項式の場合も同様であろうか？

3.4 整数の除法

整数と多項式の類似を追及するにあたって，次が基本的である（証明は省略）．

定理 3.2（除法の原理） 整数 a, b（$b \neq 0$）に対し $a = qb + r$ となる整数 q, r で $0 \leq r < |b|$ となるものが一意的に存在する．

これより（本来の）ユークリッドの互除法ができる．前回の多項式の場合の証明をなぞれば，次が示せる．

定理 3.3 整数 a, b に対し，非負の最大公約数 d が一意的に存在する．また，$ax + by = d$ を満たす整数 x, y が存在する．

$d = 1$ のとき a, b は**互いに素**であるという．

系 3.1 整数 a, b, c に対し，方程式 $ax + by = c$ が整数解をもつための必要十分条件は，c が a, b の最大公約数 d で割り切れることである．

証明 解をもつとすると，左辺は a, b の任意の公約数で割り切れるから，c も割り切れる．逆に，k を整数として $c = dk$ と書けたとする．前定理より $ax + by = d$ を満たす整数 x, y が存在するから，両辺を k 倍すればよい．□

問題 3.3 $19x + 7y = 1$ の整数解をすべて求めよ．

解答 ユークリッドの互除法により，$19 = 7 \times 2 + 5$, $7 = 5 \times 1 + 2$, $5 = 2 \times 2 + 1$．よって 19 と 7 の最大公約数は 1 である．逆に解いていくと，$1 = 5 - 2 \times 2 = 5 - (7 - 5 \times 1) \times 2 = 7 \times (-2) + 5 \times 3 = 7 \times (-2) + (19 - 7 \times 2) \times 3 = 19 \times 3 + 7 \times (-8)$．特殊解として $(x, y) = (3, -8)$ が存在する．$(x', y') = (x, y) - (3, -8)$ とおくと，$19x' + 7y' = 0$．$19x' = -7y'$ の右辺は 7 の倍数であり 19 と 7 は互いに素であるから[注3]，$x' = 7n$（n は整数）と表せる．このとき $y' = -19n$ である．逆にこれらは $19x' + 7y' = 0$ を満たす．よって解は $(x, y) = n(7, -19) + (3, -8)$（$n$ は任意の整数）．□

注3　素因数分解の一意性を使わないなら，両辺を 3 倍して $57x' = x' + 7(8x')$ を使えばよい．

3.5 整数の合同

まず，整数の場合に，余りの全体に代数構造が入ることを見ておこう．

n を整数とする．整数 a, b に対し，n による余りが等しいことは，差 $b - a$ が n の倍数になることと同値である．このとき，a と b は n を**法として合同**であるといい，記号で $a \equiv b \mod n$ と書く．以下，n を固定して考えているときは $\mathrm{mod}\, n$ を省略する．

$$a \equiv b \iff \exists k \in \boldsymbol{Z},\ b - a = kn.$$

命題 3.1 次が成り立つ．(1) $a \equiv a$, (2) $a \equiv b$ ならば $b \equiv a$, (3) $a \equiv b$ かつ $b \equiv c$ ならば $a \equiv c$, (4) $a \equiv a', b \equiv b'$ ならば，$a + b \equiv a' + b'$, $ab \equiv a'b'$．

証明 一番複雑な (4) の積のみ示し，あとは読者に任せよう．$a' = a + kn, b' = b + ln$（$k, l \in \boldsymbol{Z}$）とおくと，$a'b' - ab = (a + kn)(b + ln) - ab = (al + kb + kln)n$

となり，$al + kb + kln \in \boldsymbol{Z}$ である． □

注意 3.3 (1), (2), (3) により $\equiv$ は同値関係になる．(4) により余りの全体 $\boldsymbol{Z}/n\boldsymbol{Z}$ には代表元の取り方によらず和と積が定義され，1 をもつ可換環になる．

注意 3.4 整数の合同は暦など日常生活でも現れる．映画『サマーウォーズ』では主人公の健二が「モジュロ演算」で曜日を求める場面があった．曜日の速算法としては，コンウェイ（Conway）による「終末日規則」(Doomsday rule) がある．4/4, 6/6, 8/8, 10/10, 12/12 など特定の日が同じ曜日になることを用いる．ただしこれらの例でも「土曜と日曜の和」などは考えない．

3.6 環とイデアル

除法の原理のように，多項式と整数は多くの性質を共通にもつ．統一的に述べるために環とイデアルの言葉を使うことにする．詳細は代数学のテキストを参照されたい．

R を環とする．今回は乗法の単位元 1 をもつ可換環のみ考える．

R の部分集合 $S = \{a_1, \ldots, a_n\}$ に対し，S の元の R 係数の一次結合全体を $(a_1, \ldots, a_n)$ で表し，S で生成される**イデアル**という．例えば，$(0) = \{0\}$ であり，$(1) = R$ である．n の倍数の全体 $n\boldsymbol{Z}$ は $\boldsymbol{Z}$ の中で n で生成されるイデアルである．

I を R のイデアルとする．整数の合同と同様にして，次がわかる．R の元 a, b に対し差 $b - a$ が I に入るという関係が同値関係になる．同値類の全体は代表元の演算により自然に（1 をもつ可換）環になる．これを I による**剰余環**といい R/I で表す．

イデアルにも和・積が定義される．I, J をイデアルとするとき，I の生成元と J の生成元の和（積）たちで生成されるイデアルを，I と J の**和**（**積**）という．和のほうは I の元と J の元の和全体と一致する．系 3.1 は $a\boldsymbol{Z} + b\boldsymbol{Z}$ が $d\boldsymbol{Z}$ と書けることを述べている．

R, S を環とする．写像 $\varphi : R \to S$ が (1 をもつ環の) **準同型**であるとは，任意の R の元 r, r' に対し，$\varphi(1) = 1$, $\varphi(r+r') = \varphi(r)+\varphi(r')$, $\varphi(rr') = \varphi(r)\varphi(r')$ を満たすことをいう．例えば，余りを対応させる写像 $\boldsymbol{Z} \to \boldsymbol{Z}/n\boldsymbol{Z}$ は準同型である．全単射準同型は逆写像も準同型になり，**同型**と呼ばれる．

φ が準同型のとき，$\varphi(r - r') = \varphi(r) - \varphi(r')$ が成り立ち（$(r - r') + r' = r$ を用いよ），$\varphi(0) = 0$ が成り立つ（$\varphi(0) = \varphi(1 - 1) = \varphi(1) - \varphi(1) = 0$）．

φ で移ってくる元の全体 $\{\varphi(r) \in S \mid r \in R\}$ を φ の**像** (image) といい，$\mathrm{im}\,\varphi$ で表す．$\mathrm{im}\,\varphi$ は S の部分環になる．φ で 0 に移る元の全体 $\{r \in R \mid \varphi(r) = 0\}$ を φ の**核**（kernel）といい，$\ker\varphi$ で表す．$\ker\varphi$ は R のイデアルになる．

定理 3.4（準同型定理） $R/\ker\varphi$ は，代表元の φ による像を与える写像により，$\mathrm{im}\,\varphi$ に同型である．

3.7 互いに素

2つの整数 a, b が互いに素ならば，定理 3.3 より，$ax + by = 1$ となる整数 x, y が存在する．イデアルの言葉で言い換えると，$(a), (b)$ の元で和が 1 になるものがある．逆にそのような x, y が存在すれば，a, b の公約元は 1 を割り切るから，最大公約数は 1 である．よって，互いに素であることと，$(a)+(b)=(1)$ であることは同値である．これらのことは多項式に対しても前回示していた．そこで上の性質を用いて，より一般の環に「互いに素」の定義を拡張しておく．

1 をもつ可換環 R のイデアル I, J が**互いに素**であるとは，$I + J = R$ を満たすことを言う．すなわち，ある $a \in I$ と $b \in J$ が存在して，$a + b = 1$ となることをいう．

補題 3.1　I, J を互いに素なイデアルとするとき，$IJ = I \cap J$ となる．

証明　IJ が I と J に含まれるのは明らかだから $IJ \subseteq I \cap J$ である．逆を示す．互いに素であるという仮定より，$a + b = 1$ となる $a \in I, b \in J$ が存在する．任意の $c \in I \cap J$ に対し，$ac, cb \in IJ$ であるから $c = ac + cb \in IJ$．□

3.8 中国式剰余定理

余りを点での値に置き換える「剰余定理」を示したが，もう一つ，似た名前の定理がある．各点（素数）での値（余り）に分解する定理である．

有限個の環に対し，集合としての直積は成分ごとの演算で自然に環になることを注意しておく．

定理 3.5（中国式剰余定理）　$I_1, \dots, I_n$ を 1 をもつ可換環 R の互いに素なイデアルとするとき，次の同型が存在する．

$$R/I_1 \cdots I_n \cong (R/I_1) \times \cdots \times (R/I_n).$$

証明　以下 2 つの補題より $R/I_1 \cdots I_n \cong (R/I_1 \cdots I_{n-1}) \times (R/I_n)$ となる．あとは n に関する帰納法で示される．□

補題 3.2　I, J を互いに素なイデアルとするとき，次の同型が存在する．

$$R/IJ \cong R/I \times R/J.$$

証明　自然な全射準同型を並べて $\varphi : R \to R/I \times R/J$ ができる．$\ker \varphi = I \cap J$ であり，補題 3.1 よりこれは IJ に等しい．よって準同型定理より従う．□

補題 3.3　$I_1 \cdots I_{n-1}$ と I_n は互いに素である．

証明　n 以外の各 i に対し $a_i \in I_i, b_i \in I_n$ で $a_i + b_i = 1$ となるものが存在する．積をとると $(a_1 + b_1) \cdots (a_{n-1} + b_{n-1}) = 1$．これは $a_1 \cdots a_{n-1} \in I_1 \cdots I_{n-1}$ とそれ以外の元の和であるが，後者は I_n に属する．□

本来の中国式剰余定理は $\boldsymbol{Z}$ に関するものである．7, 5, 3 だけでなく，互いに素であれば同様の数当てが成立する．

体 K 上の多項式環 $K[x]$ においては，$\alpha \neq \alpha'$ のとき $(x - \alpha)^m$ と $(x - \alpha')^{m'}$

は互いに素である．よって，中国式剰余定理より次がわかる．

系 3.2 $\alpha_1, \ldots, \alpha_k \in K$ は相異なるとし，$m_1, \ldots, m_k$ を正の整数とする．$f(x) = (x-\alpha_1)^{m_1} \cdots (x-\alpha_k)^{m_k} \in K[x]$ に対し次の同型がある．

$$K[x]/(f(x)) \cong K[x]/((x-\alpha_1)^{m_1}) \times \cdots \times K[x]/((x-\alpha_k)^{m_k}).$$

まとめると，次数が $f(x)$ より小さい多項式は，$f(x)$ で割った余りを通じて，中国式剰余定理により，因子 $(x-\alpha_i)^{m_i}$ たちで割った余りの組と，一対一対応する．後者は一般化された剰余定理によって，α_i における $m_i - 1$ 次までの微分係数で決まる．以上で，$d+1$（$=\deg f$）個分の剰余の条件を与えたとき，高々 d 次で条件を満たす多項式が唯一つ存在することが示された．

これで理論的にはすっきりしたが，実際に各因子による余りから $f(x)$ による余りを求めてみよ，と言われると，上の証明からでは最大公約元を繰り返し求めることになる．諦めて連立 1 次方程式を解いてもよいが，次の方法もある．

3.9 ラグランジュの補間公式

$d+1$ 個の点での値が指定されると，それを満たす高々 d 次の多項式を書き下す公式がある．

文字 x に関する d 次以下の多項式は，単項式 $1, x, x^2, \ldots, x^d$ の一次結合として一意的に表され，その全体 P_d は $d+1$ 次元の線形空間をなす．

さて，α_i（$0 \le i \le d$）を相異なる $d+1$ 個の実数とする．i ごとに d 次式

$$l_i(x) := \prod_{j \neq i} \frac{x-\alpha_j}{\alpha_i - \alpha_j}$$

を定める．$l_i(\alpha_j) = \delta_{ij}$ である[注4]．$l_i(x)$ を**ラグランジュ（Lagrange）多項式**という．

注4　δ_{ij} は，$i=j$ のとき 1，$i \neq j$ のとき 0 を表し，**クロネッカー**（Kronecker）**のデルタ**と呼ばれる．

命題 3.2 $l_0(x), \ldots, l_d(x)$ は P_d の基底である．

証明　個数 $d+1$ が P_d の次元と一致しているので，一次独立であることを示せばよい．多項式として $\sum_{i=0}^{d} c_i l_i(x) = 0$ が成り立ったとする．$x = \alpha_i$ を代入すると $c_i = 0$ を得る．よって $l_0(x), \ldots, l_d(x)$ は一次独立である． □

特に，任意の $f(x) \in P_d$ は $l_i(x)$ たちの一次結合として一意的に表せる．これが実に簡単なのである．$f(x) = \sum_{i=0}^{d} c_i l_i(x)$ であるとすると，$x = \alpha_i$ を代入して，$f(\alpha_i) = c_i$ が従う．よって次を得た．

定理 3.6（ラグランジュの補間公式） 相異なる実数 $\alpha_0, \ldots, \alpha_d$ での値がそれぞれ $f(\alpha_0), \ldots, f(\alpha_d)$ となる高々 d 次の実数係数多項式が唯一つ存在し，次で与えられる．

$$f(\alpha_0) l_0(x) + \cdots + f(\alpha_d) l_d(x).$$

注意 3.5 $f(x) \in P_d$ でなければ，もとの $f(x)$ とは異なる．

今回の問題 3.1 では，最初から $f(x)$ が 3 次以下の多項式としているので，一意性より補間によりできた多項式と一致する．

問題 3.1 の別解　ラグランジュの補間公式により $f(x)=f(0)\frac{(x-1)(x-2)(x-3)}{(0-1)(0-2)(0-3)}+f(1)\frac{x(x-2)(x-3)}{(1-0)(1-2)(1-3)}+f(2)\frac{x(x-1)(x-3)}{(2-0)(2-1)(2-3)}+f(3)\frac{x(x-1)(x-2)}{(3-0)(3-1)(3-2)}=-\frac{1}{3}(x^3-6x^2+11x-6)+(x^3-5x^2+6x)+(x^3-4x^2+3x)+\frac{4}{3}(x^3-3x^2+2x)$ $=3x^3-11x^2+8x+2$. □

注意 3.6　関数と多項式の違いについて注意しておく.

2つの多項式 $f(x), g(x)$ が多項式として（すなわち，式の変形により）等しければ，もちろん関数としても（すなわち，任意の x の値に対して恒等的に）等しい．変数の値を代入してから同じ式変形をすれば，関数の値も等しくなるからである．しかし，逆は一般には慎重になる必要がある．

実数は無限集合なので，次の命題により，2つの実数係数多項式が $\boldsymbol{R}$ 上の関数として恒等的に等しければ多項式としても等しい．しかし，世の中には有限個の元からなる体もあり，その場合，多項式関数の式としての表示は一意的とは限らない．例えば $\boldsymbol{Z}/2\boldsymbol{Z}$ 上の関数としては x^2 と x は同じである．

命題 3.3　K を体とし，$f(x), g(x)$ を高々 d 次の K 係数多項式とする．相異なる $d+1$ 個の値 $\alpha_0,\dots,\alpha_d\in K$ に対し $f(\alpha_i)=g(\alpha_i)$ $(0\le i\le d)$ となるならば，多項式として $f(x)=g(x)$ である．

証明　差 $g(x)-f(x)$ は高々 d 次の多項式である．α_i $(0\le i\le d)$ を代入して 0 となるから，因数定理を繰り返し用いて $(x-\alpha_0)\cdots(x-\alpha_d)$ で割り切れる．次数を比較して $g(x)-f(x)=0$. □

注意 3.7　ヴァンデルモンドの行列式が差積になることを知っていれば，問題 3.1 の解答のように解いて係数行列が正則になることからも示せる．

問題 3.4　$f(x)$ を高々2次の実数係数多項式，α, β, γ を相異なる実数とする．$\boldsymbol{R}\setminus\{\alpha, \beta, \gamma\}$ を定義域とする次の有理関数を部分分数に分解せよ．

$$\frac{f(x)}{(x-\alpha)(x-\beta)(x-\gamma)}.$$

解答　未定係数 A, B, C を用いて

$$\frac{f(x)}{(x-\alpha)(x-\beta)(x-\gamma)}=\frac{A}{x-\alpha}+\frac{B}{x-\beta}+\frac{C}{x-\gamma}$$

とおく．$x\neq\alpha,\beta,\gamma$ では $(x-\alpha)(x-\beta)(x-\gamma)\neq 0$ を掛けても同値であり，$f(x)=A(x-\beta)(x-\gamma)+B(x-\alpha)(x-\gamma)+C(x-\beta)(x-\gamma)$ が成り立つ．実数は無限集合であるから，α, β, γ 以外に少なくとも3つの値で両辺は一致する．よって高々2次の多項式としても両辺は等しいので，実数全体の上の関数としても等しい．$x=\alpha, \beta, \gamma$ を代入して A, B, C が定まり，求める部分分数展開は次で与えられる．

$$\frac{f(\alpha)}{(\alpha-\beta)(\alpha-\gamma)}\frac{1}{x-\alpha}+\frac{f(\beta)}{(\beta-\alpha)(\beta-\gamma)}\frac{1}{x-\beta}+\frac{f(\gamma)}{(\gamma-\alpha)(\gamma-\beta)}\frac{1}{x-\gamma}.$$ □

別解　ラグランジュの補間公式より恒等式

$$f(x)=f(\alpha)\frac{(x-\beta)(x-\gamma)}{(\alpha-\beta)(\alpha-\gamma)}+f(\beta)\frac{(x-\alpha)(x-\gamma)}{(\beta-\alpha)(\beta-\gamma)}+f(\gamma)\frac{(x-\alpha)(x-\beta)}{(\gamma-\alpha)(\gamma-\beta)}$$

を得る．$(x-\alpha)(x-\beta)(x-\gamma)$ で割ればよい． □

次の問題は正方行列のべき乗の計算等に応用できる（最小多項式等で割る）．

問題 3.5　α, β, γ を相異なる実数とする．x^n を $(x-\alpha)(x-\beta)(x-\gamma)$ で割った余りを求めよ．

余りを ax^2+bx+c のようにおいて求めても構わないが，即座に書き下せる．

解答　商を $q(x)$，余りを $r(x)$ とする．$r(x)$ は高々 2 次式である．$x^n = (x-\alpha)(x-\beta)(x-\gamma)q(x)+r(x)$ より $r(\alpha)=\alpha^n$, $r(\beta)=\beta^n$, $r(\gamma)=\gamma^n$ であるから，ラグランジュの補間公式より $r(x)$ は次の通り．

$$\alpha^n\frac{(x-\beta)(x-\gamma)}{(\alpha-\beta)(\alpha-\gamma)}+\beta^n\frac{(x-\alpha)(x-\gamma)}{(\beta-\alpha)(\beta-\gamma)}+\gamma^n\frac{(x-\alpha)(x-\beta)}{(\gamma-\alpha)(\gamma-\beta)}.$$ □

注意 3.8　もちろん整理すれば x, α, β, γ についての多項式になる．

例題 3.1 は割る多項式に重根があるが，部分分数展開の計算をヒントにする．

例題 3.1 の解答　$\boldsymbol{R}[x]$ の中で 3 次以下の多項式全体のなす集合 P_3 は，4 次元の部分空間である．$p_0(x) = (x-1)^2(x-2)$, $p_1(x) = x(x-2)$, $p_2(x)=x(x-1)(x-2)$, $p_3(x)=x(x-1)^2$ とおく．式として $\sum_{i=0}^{3} c_ip_i(x)=0$ $(c_0,\ldots,c_3\in\boldsymbol{R})$ とする．$x=0,1,2$ を代入して $c_0=c_1=c_3=0$ がわかる．$p_2(x)\neq 0$ であるから $c_2=0$ である．よって $p_0(x),\ldots,p_3(x)$ は一次独立であるから P_3 の基底である．改めて $f(x)=\sum_{i=0}^{3} c_ip_i(x)$ とおく．$x=0,1,2$ を代入して $f(0)=-2c_0$, $f(1)=-c_1$, $f(2)=2c_3$．また，微分した式に $x=1$ を代入すると，もともと $(x-1)^2$ で割れる式は 0 になるから，$f'(1)=-c_2$．よって $f(x)=p_0(x)+2p_1(x)+2p_3(x)=3x^3-6x^2+3x-2$. □

3.10 多変数への拡張

例題では 1 変数の場合を扱ったが，多変数にも自然に拡張される．

問題 3.6　K を体とする．相異なる 5 点 $(\alpha_i, \beta_i)\in K^2$ $(1\leq i\leq 5)$ に対し，K 上の 2 変数 2 次式 $f(x,y)$ で，式として 0 でないが，$f(\alpha_i, \beta_i)=0$ $(1\leq i\leq 5)$ となるものが存在することを示せ．

解答　2 次式は一般に $f(x,y)=ax^2+by^2+hxy+kx+ly+c$ $(a, b, h, k, l, c\in K)$ とおける．(α_i, β_i) たちで 0 となる条件は，a, b, h, k, l, c に関する同次連立 1 次方程式である．5 つの式しかないから，階数は高々 5 である．階数が未知数の個数 6 より真に小さいので，自明でない解をもつ． □

注意 3.9　ただし，もはや一意性は一般には成り立たず，点の配置による．例えば 5 点が同一直線上にあると，その直線と，任意の直線から $f(x,y)$ が作れる．ここから代数幾何の精妙な世界が広がっていく．

参考文献

1)　吉田光由（大矢真一校注），『塵劫記』，岩波文庫青 24–1，岩波書店，1977.

（こばやし・まさのり，首都大学東京大学院理工学研究科）

リレー連載

フィールズ賞で語る現代数学

第5回

代数幾何学(1)

代数幾何学の再構築

前田 博信

1. はじめに

1954 年にフィールズ賞を受賞した小平邦彦とセールは代数幾何学の分野に層のコホモロジーを応用して成果をあげ，1966 年にフィールズ賞を受賞したグローテンディックは圏論的な代数幾何学，すなわちスキーム論を創世した．そして，1970 年にフィールズ賞を受賞した廣中平祐は，スキーム論に基づいた方法で特異点解消問題を解いた．ここでは古典的な代数幾何学からスキーム論に至るまでの道のりを簡単にたどりたい．

2. 代数幾何学の故郷

私たちが最初に出会う代数多様体は円錐曲線，すなわち楕円，放物線，双曲線であろう．円錐曲線は 2 次方程式 $ax^2+2bxy+cy^2+2dx+2ey+f=0$ で記述できるので 2 次曲線ともよばれる．さて，この 2 次式を出発点にとるとすぐにいろいろな問題が考えられる[8]．例として，2 次同次式 $ax^2+2bxy+cy^2$ がこの形の式の積に分解するかどうかという問題（ガウス）を考えてみる．

しばらくの間 $a,b,c,\ldots$ は不定元としよう．今，3 つの 2 次式 $f=ax^2+2bxy+cy^2$, $f'=a'x'^2+2b'x'y'+c'y'^2$, $F=AX^2+2BXY+CY^2$ が，変数変換 $X=pxx'+p'xy'+p''yx'+p'''yy'$, $Y=qxx'+q'xy'+q''yx'+q'''yy'$ により $F=ff'$ となるとき，F は積 ff' に分解するという．

ここで $\boldsymbol{x}=\begin{pmatrix}x\\y\end{pmatrix}$, $\boldsymbol{x}'=\begin{pmatrix}x'\\y'\end{pmatrix}$, $\boldsymbol{X}=\begin{pmatrix}X\\Y\end{pmatrix}$, $\theta=\begin{pmatrix}a&b\\b&c\end{pmatrix}$, $\theta'=\begin{pmatrix}a'&b'\\b'&c'\end{pmatrix}$, $\Theta=\begin{pmatrix}A&B\\B&C\end{pmatrix}$, とおくと $f={}^t\boldsymbol{x}\theta\boldsymbol{x}$, $f'={}^t\boldsymbol{x}'\theta'\boldsymbol{x}'$, $F={}^t\boldsymbol{X}\Theta\boldsymbol{X}$ と書ける（${}^t\boldsymbol{x}$ は $\boldsymbol{x}$ の転置を表す）．

一方，変数変換も行列

$$M=\begin{pmatrix}px+p''y & p'x+p'''y\\ qx+q''y & q'x+q'''y\end{pmatrix},$$

$$M'=\begin{pmatrix}px'+p'y' & p''x'+p'''y'\\ qx'+q'y' & q''x'+q'''y'\end{pmatrix}$$

を用いて $\boldsymbol{X}=M\boldsymbol{x}'=M'\boldsymbol{x}$ と書ける．この式に左から M の余因子行列 $\widetilde{M}$ をかけると $\widetilde{M}\boldsymbol{X}=(\det M)\boldsymbol{x}'$ となり，この左辺は行列

$$L=\begin{pmatrix}q'X-p'Y & q'''X-p'''Y\\ -qX+pY & -q''X+p''Y\end{pmatrix}$$

を用いて $\widetilde{M}\boldsymbol{X}=L\boldsymbol{x}$ と書ける．

$\det(\theta)=d$, $\det(\theta')=d'$, $\det(\Theta)=D$ をそれぞれ f, f', F の行列式（Determinant）とよぶ．判別式とは符号が逆である．

$F=ff'$ すなわち ${}^t\boldsymbol{X}\Theta\boldsymbol{X}=({}^t\boldsymbol{x}\theta\boldsymbol{x})({}^t\boldsymbol{x}'\theta'\boldsymbol{x}')$

$= {}^t\boldsymbol{x}(f'\theta)\boldsymbol{x}$ の左辺は ${}^t\boldsymbol{X}\Theta\boldsymbol{X} = {}^t\boldsymbol{x}({}^tM'\Theta M')\boldsymbol{x}$ と書けるから，係数部分を比較して $f'\theta = {}^tM'\Theta M'$ を得る．両辺の行列式をとると

$$f'^2 d = D\det(M')^2 \tag{1}$$

となる．同様にして，${}^t\boldsymbol{X}\Theta\boldsymbol{X} = {}^t\boldsymbol{x}'(f\theta')\boldsymbol{x}'$ と $\boldsymbol{X} = M\boldsymbol{x}'$ により $f\theta' = {}^tM\Theta M$ が得られ，

$$f^2 d' = D\det(M)^2 \tag{2}$$

を得る．次に，${}^t\boldsymbol{x}'(f\theta')\boldsymbol{x}' = {}^t\boldsymbol{x}(f'\theta)\boldsymbol{x}$ の両辺に $\det(M)^2$ をかけて，$\det(M)\boldsymbol{x}' = L\boldsymbol{x}$ を代入すると $\det(M)^2 f'\theta = {}^tL(f\theta')L$ が得られる．行列式をとり，式 (1), (2) を用いると

$$F^2 dd' = D^2\det(L)^2 \tag{3}$$

が得られる．

最後に $\det(M), \det(M'), \det(L)$ を計算する．$P = pq' - qp'$, $Q = pq'' - qp''$, $R = pq''' - qp'''$, $S = p'q'' - q'p''$, $T = p'q''' - q'p'''$, $U = p''q''' - q''p'''$, $V = qq''' - q'q''$, $W = p'q'' + q'p'' - pq''' - qp'''$, $Z = pp''' - p'p''$ とおくと，

$$\det(L) = VX^2 + WXY + ZY^2,$$
$$\det(M) = Px^2 + (R-S)xy + Uy^2,$$
$$\det(M') = Qx'^2 + (R+S)x'y' + Ty'^2,$$
$$\det(L) = -\det(M)\det(M')$$

となり，必要な式がそろった．

式 (1) より，d/D は平方元であるから $d/D = n^2$ とおく．標数が 2 でなければ n は 2 つあるから 1 つ決めておく．同様に $d'/D = n'^2$ となる n' を 1 つ決めておく．

以上から次のことが分かる．$F = ff'$ となるためには，d'/d が平方元であり，$d'/D = n'^2$, $d/D = n^2$ となる n, n' が存在して，$P = an'$, $R - S = 2bn'$, $U = cn'$, $Q = a'n$, $R + S = 2b'n$, $T = c'n$, $Ann' = -V$, $2Bnn' = -W$, $Cnn' = -Z$ となるような $p, p', p'', p''', q, q', q'', q'''$ が存在すればよい．

特に，a, b, c, a', b', c' がすべて整数のとき，有理数 n, n' を $d'/d = (n'/n)^2$ であって，na', $n2b'$, nc', $n'a$, $n'2b$, $n'c$ がすべて整数で，それらの最大公約数が 1 となるように選ぶことができれば，$P = an'$, $R - S = 2bn'$, $U = cn'$, $Q = a'n$, $R + S = 2b'n$, $T = c'n$ を満たす整数 p, p', p'', p''', q, q', q'', q''' を線形代数の計算で求めることができる．このとき，$Ann' = -V$, $2Bnn' = -W$, $Cnn' = -Z$ を満たす整数 A, B, C が定まり，F が ff' に分解する．このような F を f と f' の合成[10]という．

例として，$f = x^2 - 2xy - 2y^2$, $f' = 3x'^2 - 6x'y' - y'^2$ の合成を計算しよう．$d = -3$, $d' = -12$ である．$d'/d = 2^2$ であるから，$n = 1$, $n' = 2$ とすると，$na' = 3$, $n2b' = -6$, $nc' = -1$, $n'a = 2$, $n'2b = -4$, $n'c = -4$ の最大公約数は 1 である．したがって $(P, Q, R, S, T, U) = (2, 3, -5, -1, -1, -4)$ をプリュッカー座標とする直線上の整数座標の 2 点を計算し，例えば，$(p, p', p'', p''') = (4, 2, 5, -3)$, $(q, q', q'', q''') = (-3, -1, -3, 1)$ を選ぶことができる．このとき $V = -6, W = -24, Z = -22$ となるから，$F = 3X^2 + 12XY + 11Y^2$ が f と f' の合成の 1 つである．

代数幾何学の故郷であり，現在でもまだ未解決問題が残る 2 次式の古典理論[7]には，代数多様体という概念はまだ現れていない．しかし，行列式が活躍することに注目しよう．行列式は線形変換のオイラー標数といってもよく，オイラー標数は交点理論やリーマン・ロッホの定理を典型として代数幾何学のさまざまな分野に現れる．

3. 代数曲線とリーマン・ロッホの定理

私たちが 2 次曲線の次に出会う代数多様体は 2 次曲面か 3 次曲線であろう．2 次曲面は比較的私たちの身近に存在する．例えば，ガスタンクの形は真の球面である．また，南ドイツのガーヒング市にある原子炉建屋の形は回転楕円半面をしていて，通称，原子卵（アトームアイ）とよばれ，市の紋章（ワッペン）にも描かれているし，神戸ポートタワーの形は一葉双曲面である．

余談はさておき，もう一方の 3 次曲線は，その

数学的理論が驚くほど内容豊富で，モジュライ空間，アーベル多様体，ファイバー空間，特異点解消など，代数幾何学のほとんどすべての分野の原型を含んでいる．

3 次曲線の分類はニュートンにさかのぼるといわれ，方程式から出発する研究の元祖とみなされている．ところが，式の計算を積み上げるよりも式の背後にある空間的実体や理念を研究するほうが理解が深まる，ということに気づいたのが天才リーマンである[5)]．リーマンの 1 変数代数関数論，すなわち閉リーマン面の理論をきっかけとして，一般の代数曲線や代数曲面の解析的あるいは幾何学的な性質の研究が進むことになる．

そこで，今度はリーマン面を出発点にとる．C をコンパクトな 1 次元複素多様体, すなわち閉リーマン面とする．C は位相的には球面にハンドルが p 個ついた曲面であり，p を C の種数とよぶ．

最初の重要な成果として，C 上に定数以外の有理型関数が存在することが証明される．これを用いて C からリーマン球面への全射正則写像（被覆写像）が定まり，被覆面としての次数 n と，重複度をこめた分岐点の個数 w が決まり，

$$p = \frac{w}{2} - n + 1$$

が成り立つ．別の有理型関数（被覆写像）を選んでもこの形の式が成り立ち，リーマンの公式という．

複素数における 3 次曲線はワイエルシュトラスのペー関数 $\wp(z)$ により, 4 点で分岐する 2 次の被覆面として実現される．したがって $p = 4/2-2+1 = 1$ が 3 次曲線の種数である．なお，リーマンは最初，分岐点を旋回点（Windungspunkt）とよんでいた．点の周りを何回かぐるぐる回って元に戻るからである．

次に，$D = \sum m_j P_j$ を C 上の因子とする．C 上の有理型関数 f であって，その因子 (f) が $(f) + D \geqq 0$ を満たすもの全体に 0 を加えたものを $L(D)$ とおくと，$L(D)$ は有限次元ベクトル空間となる．その次元を $l(D)$ とすると，どんな D についても $l(D) \geqq \deg D + 1 - p$ が成り立ち，リーマンの不等式とよばれる．

等式を得るには微分が必要である．C 上の微分 ω の因子を $H = (\omega)$ とすると，どんな D についても

$$l(D) - l(H - D) = \deg D + 1 - p$$

が成り立つ．これが有名なリーマン・ロッホの定理である．この結果を拡張することが代数幾何学の課題の 1 つとなり，1950 年代に代数幾何学に層のコホモロジーが導入されるきっかけになる．

さて，ここで視点を変えて，今度はリーマン面上の関数に注目しよう．C 上の有理型関数の全体 K は体（たい）という構造をもつ無限集合をなし，C からリーマン球面への被覆写像を 1 つ決めると，K は有理関数体 $\mathbb{C}(z)$ の n 次拡大体となる．この拡大に関する分岐を代数的に定義できれば複素係数以外の代数関数体についても n と w が定まり，したがってリーマンの公式を用いて K の種数 p が定義できることになる．

改めて，k を一般の体とする．不完全体でもよい．K を有理関数体 $P = k(z)$ の n 次拡大体とする．最初の目標は K のリーマン面，すなわちその上の有理関数の全体が K となるような空間的実体を定義することである．リーマンの後輩であったデデキントは K の中の素イデアルの適当な集合を K のリーマン面と定義したが, k が無限体で K/P が非分離な場合は無限個の素イデアルが分岐することがあるためリーマンの公式が使えない．その代わりに K/P の素因子（離散付値）の集合としてリーマン面 C を定義するとうまくいく．

付値を用いると代数関数体 K/P のリーマン面のみならず，その標準因子 H や種数 p も定義できる．$L(D)$ は K の中の加群とみなされ，その次元 $l(D)$ と次数（実は行列式）$\deg(D)$ を計算するとリーマン・ロッホの式が成り立つことが代数的に証明できる[5)]．

このアイデアは後にザリスキによって一般化された．ザリスキは高次元の代数関数体の中の離散とは限らない付値も全部集めた空間をリーマン空間とよび, 2 次元と 3 次元の特異点解消の証明に応用した．このリーマン空間は永田雅宜による代数

多様体の完備化の証明にも用いられた．なお，一般付値の理論は整数論から借用したものであって，整数論では巡回拡大でないアーベル拡大や無限次拡大の構成などに用いられる．

4. イタリア学派の代数曲面論

代数曲面の研究は，20 世紀前半に，イタリア学派とよばれる数学者たち，カステルヌオーヴォやエンリケスやセヴェリ等により大きく発展した．その成果の 1 つが，代数曲面の双有理的分類理論である．しかし，当時の代数幾何学は定義や証明が厳密でなく，イタリア学派は多くの重要な成果をあげたにも関わらず，次第に不確実な定理が増えてしまい，袋小路に入り込んでしまったといわれる．

代数曲面の研究では代数曲線の場合には意識されなかった新しい問題が現れてくる．S をコンパクトな 2 次元の複素多様体として出発しようとすると，1 次元の場合と違い，これだけでは有理型関数が存在しない．そこで S は最初から射影空間の中の既約な超曲面とする．ただし，S は一般に特異点をもつ．平面代数曲線がクレモナ変換により通常特異点しかもたないように変換できたように，代数曲面も高々通常特異点しかもたないようにしておく．なお，特異点解消問題が解けている現在では S の非特異モデル $\widetilde{S}$ を考察するのが普通であるが，しばらくの間，S は射影空間の中の d 次超曲面としよう．

S 上の素因子とは，特異点もあるかもしれない既約代数曲線 C のことであり，これらの整数係数の結合 D が因子である．S は射影空間の中にいるから別の超曲面との交点集合も因子になる．このような因子を有効であるという．D と有理関数の因子の差しか違わない因子 D' は D と線形同値であるという．D と線形同値な有効な因子の全体を D の完備線形系といい $|D|$ と書く．$|D|$ は $L(D)-\{0\}$ を定数倍という同値関係で割った射影空間の構造をもち，S の射影空間における性質を反映する重要な集合である．代数曲面上のリーマン・ロッホの式も，代数曲線の場合と同様に，$\dim|D| = l(D)-1$ を求められる式のことである．

まず S の種数を定めよう．曲線の場合と同様に，標準因子，すなわち微分因子 K の次元 $l(K) = p_g$ を幾何種数という．S は射影空間の中にいるから，S の標準因子 K は S が非特異であれば $d-4$ 次の超曲面が定める因子と一致する．このときは，$\dim L(K)+1$ は S の射影空間におけるヒルベルト多項式 $H(t)$ の定数項 $H(0)$ と一致する．そこで一般の S も不変量 $H(0)-1$ を p_a とおき，S の算術種数という．実際には $p_g \geqq p_a$ であり，その差 q は不正則数とよばれた．

これらの不変量の意味は，代数幾何学に層のコホモロジーが導入された 1950 年以降に明らかになった．現在では，$H(0)$ は交代和 $\dim H^2(\mathcal{O}_S) - \dim H^1(\mathcal{O}_S) + \dim H^0(\mathcal{O}_S)$ に等しいことが分かり，セールの双対定理により $\dim H^2(\mathcal{O}_S) = p_g$ も分かるから q の正体は $\dim H^1(\mathcal{O}_S)$ であることが分かる．

さて，代数曲面上のリーマン・ロッホの式には 2 つの因子 D と $D-K$ の交点数 $D\cdot(D-K)$ が現れる．ところが，20 世紀前半では交点数の理論も不十分で，満足のいく定義は 20 世紀後半になるまで得られなかった．

例えば，ある特異 4 次曲面 V と直線 W が 1 点 Z で交わり，その交点数をイデアルの長さで計算すると 5 になる例（ファン・デル・ヴェルデン）がある．4 次と 1 次が 1 点で交わり，その交点重複度が $4\times 1=4$ にならないとベズーの定理が成立しない．この例をきっかけにしてファン・デル・ヴェルデンはイデアル論を代数幾何学の基礎にすることをやめて，より古典的な消去法を基礎とする代数幾何学を構築した．

この例の本質を鮮やかに解明したのはセールである．セールは交点数をオイラー標数，すなわち交代和 $I(V,W;Z) = \sum(-1)^i \dim \mathrm{Tor}_i^Z(V,W)$ として定義[9]し，上の例では $I=5-1=4$ がベズーの式になることを示した．

このような状況にも関わらず，イタリア学派は S 上の因子 D についてリーマン・ロッホの不等式

$$l(D)+l(K-D) \geqq \frac{D\cdot(D-K)}{2}+1+p_a$$

を示し，これが等式

$$l(D)-s(D)+l(K-D) = \frac{D\cdot(D-K)}{2}+1+p_a$$

となるようにした補正項 $s(D)$ を超過数（superabundance）とよび，その評価を研究した．層のコホモロジーを用いなかった当時の研究は一つ一つ例を計算して結果を確認するという困難な仕事であった．ザリスキはイタリア学派の代数曲面論の成果[11]を 1935 年に英語で発表したが，代数幾何学の基礎が脆弱であることも広く知られるようになった．

5. 代数幾何学の変貌

リーマン面を高次元に一般化した複素多様体の定義は 1913 年出版のワイルの『リーマン面の理念』をそのまま高次元化すればよかったが，代数多様体の代数的な定義は 1960 年頃まで決定版が存在せず，研究分野ごとに都合のよい定義が流行し，混乱した．スキーム論が出現するまでの代数多様体の代数的定義で代表的なものはヴェイユとザリスキによるものである．

ヴェイユは万有体という巨大な代数閉体を基礎体とする絶対既約な代数多様体を用いた．生成点の特殊化という古典的な方法で交点理論を展開し，有理点の個数を計算して合同ゼータ関数のリーマン予想の類似を解くことに成功した．しかし，ヴェイユの定義では非特異点が絶対非特異点となるため，特異点の精密な研究には向かなかった．

ザリスキは一般の体を基礎体とする代数関数体を１つ決めて，その中の有限型のアフィン環の集まりとして代数多様体を定義した．集めたものがコンパクトであるかどうかは代数関数体の付値を用いて判定された．また，単項変換のような双有理変換は代数関数体の中で，例外因子の点に相当する局所環を追加することで定義された．

双有理幾何学では関数体が固定されるのでこれでもよかったが，別の関数体との関係を扱うには不便であった．しかし，基礎体を一般にしたため古典的な代数幾何学の定義を見直すきっかけにもなった．例えば，3 元体 $\mathbb{F}_3$ 上の有理関数体 $\mathbb{F}_3(t)$ を基礎体とする 3 次曲線 $y^2=x^3-t$ は種数が 1 であるが，3 次拡大 $\mathbb{F}_3(t)[\tau]/(\tau^3-t)$ をすると種数が 0 の曲線 $y^2=(x-\tau)^3$ になるから，種数の定義をし直さなくてはならない．

このような混乱した状況は 1950 年代後半にグローテンディックがスキームの言葉で代数幾何学の基礎理論[1]を構築したことにより収まり，それまでの様々な定義はスキームの言葉で分かりやすく再定義[2]できるようになった．スキームには位相と層がついているので，スキーム論における定義は純粋に代数的な定義とは言えなくなったが，逆に幾何学的直観に近くなり適用範囲が広がった．

例えば，スキームの次元は，スキームの位相による閉集合の組成列の長さを用いて定義される．これは有限生成というような条件がなくてもよい．例えば，代数的スキーム X の余次元 1 の非特異点 P における局所環の完備化 A を考える．A は 1 変数べき級数環 $k[[t]]$ であるが，k 上の超越次数が無限大であるから，Spec$A$ の次元を純代数的に定義するのは難しい．しかし，Spec$A$ には空でない閉集合が 2 つしかなく，スキームとしての次元は 1 となり幾何学的な直観と合う．

6. セールと小平邦彦

スキーム論のきっかけとなったのは圏論的に整備されたホモロジー代数学と層の理論であった．層のコホモロジーが代数幾何学に取り入れられたのは 1950 年代前半で，それまで停滞していた高次元のリーマン・ロッホの定理の研究に本質的な進歩をもたらした．

n 次元代数多様体 X 上の因子 D のリーマン・ロッホの定理は，D の次元 $l(D)$ ではなく，D のオイラー標数，すなわち交代和 $\chi(D)=\sum_{i=0}^{d}(-1)^i \dim H^i(\mathcal{O}(D))$ を表す式である，というのがセールのアイデアである．

このとき，リーマン・ロッホの式は D のチャー

ン類 $\mathrm{ch}(\mathcal{O}(D))$ と接束 $\mathcal{T}_X$ のトッド類 $\mathrm{td}(\mathcal{T}_X)$ を用いて

$$\chi(D) = (\mathrm{ch}(\mathcal{O}(D)) \cdot \mathrm{td}(\mathcal{T}))_n$$

と書ける．このリーマン・ロッホの定理は一般のベクトル束 $\mathcal{E}$ の場合に拡張されて，ヒルツェブルフ[4]によって証明された．

同じ頃，セールは双対定理

$$H^i(\mathcal{O}(D)) \cong H^{n-i}(\mathcal{O}(K-D))$$

を証明し，さらに小平はいわゆる小平消滅定理

$$H^i(\mathcal{O}(K+F)) = 0 \quad (i > 0, F \text{ は豊富})$$

を証明した．これらの定理を用いると，必要としていた $l(D)$ を求めることができる．

リーマン・ロッホの定理はその後さらに一般化された．グローテンディックは視点を変え，ベクトル束を，より一般の連接層に拡張し，1つの代数多様体ではなく代数多様体の間の正則写像 $f : X \to Y$ に対してリーマン・ロッホの定理を拡張した．適当な同値関係を省略して述べると，f が固有正則写像で $\mathcal{F}$ が X 上の連接層のとき，交代和 $\sum_{j\geq 0}(-1)^j R^j f_* \mathcal{F}$ を $f_! \mathcal{F}$ と表すと

$$\mathrm{ch}(f_! \mathcal{F}) = f_*(\mathrm{ch}(\mathcal{F}) \cdot \mathrm{td}(\mathcal{T}_{X/Y}))$$

が成り立ち，グローテンディック・リーマン・ロッホの定理という．

ベクトル束を，一般の連接層へ拡張する，というように，より広い枠組みで定式化するのは現代数学の特徴であろう．身近な例として，ヘヴィサイド関数は普通の関数としては微分できないが，超関数としてならいくらでも微分できる．

層はもともと多変数複素関数論の研究において岡潔によって導入されたものであったが，今日ではいろいろな分野で使われる現代数学の代表的な道具である．1954年にアムステルダムでセールと共にフィールズ賞を受賞した小平は受賞前後から層を用いた研究で多くの成果をあげている．特に，小平とスペンサーによる複素多様体の変形理論は層の言葉が不可欠である．

小平の論文集[6]の第I巻には層を用いた論文はない．層が活躍するのは第II巻からである．小平の論文では層という用語は最初はフランス語から借用した faiseaux がそのまま使われ，次に stack となり，最後に sheaf という英語に落ち着いている．

7. グローテンディック

層のコホモロジーを代数幾何学に移植する試みは最初セールによってなされたが，より徹底して代数幾何学を基礎から作り直した数学者が1966年にモスクワでフィールズ賞を（本人不在で）受賞したグローテンディックである．彼のスキーム論に基づく代数幾何学は古くからの未解決問題を次々と解いて，その後のフィールズ賞受賞者を次々と輩出した．1970年受賞の廣中，1974年受賞のマンフォード，1978年受賞のドリーニュ，1986年受賞のファルティングスはグローテンディックから大きな影響を直接受けている．

スキームはアフィンスキームを貼り合わせたものである．アフィンスキーム $\mathrm{Spec}A$ は，単位元1をもつ可換環 A から，A 自身ともいえる構造層 $\widetilde{A}$ をもつ位相空間として定義される．A が体の上の有限生成な整域 $k[z_1, \ldots, z_n]$ であれば $\mathrm{Spec}A$ は古典的なアフィン代数多様体に非常に近い性質をもつが，一般のアフィンスキーム $\mathrm{Spec}A$ では A に特別な条件をつけなくてもよく，その利点は大きい．

例えば，代数多様体 X の点 P における局所環 $\mathcal{O}_{X,P}$ のアフィンスキーム $X' = \mathrm{Spec}(\mathcal{O}_{X,P})$ はネータースキームではあるが有限型でなく，自然な写像 $X' \to X$ は閉埋め込みでないし，開埋め込みでもない．X' には閉点が1つしかないし，P が X の閉点でないときには X' は X よりも次元が低くなる．X' は奇妙なアフィンスキームであるがブローアップの列と可換になるため役に立つ．

さらに，局所環 $\mathcal{O}_{X,P}$ を完備化して $\widehat{X} = \mathrm{Spec}(\widehat{\mathcal{O}_{X,P}})$ を考えると，X' より構造が簡単で，具体的な計算もしやすくなるが，元の X の情報が失われることがある．しかし，特異点解消を考える場合は X にエクセレント[1]という条件があ

れば，完備化しても特異点の情報が保たれる．エクセレントなスキームは特異点解消ができると予想されていて，標数零の場合は廣中によって解かれた．

8. 廣中平祐

1970 年にフランスのニースでフィールズ賞を受賞した廣中の代表的業績は標数零の代数多様体の特異点解消定理の証明[3]である．廣中は特異点解消問題を一般のエクセレントスキームの場合に拡張して，問題自体を定式化しなおし，特異性を改善するための手順自身を定義した．廣中の証明は複雑ではあるが，標数零の仮定を用いた箇所が明確に分かるようになっている．

廣中の単項変換（ブローアップ）は，イデアルの連接層を単項イデアルの層に変換するような普遍的な変換として定義される．ザリスキの定義と異なり，代数関数体を必要としない．そのため整数論にも応用できる．

例えば，4 次式 $f = x^4 - x^3 + x^2 - 2x + 4$ を考える．f の判別式は $11492 = 2^2 \cdot 13^2 \cdot 17$ である．$V = \mathrm{Spec}(\mathbb{Z}[x]/(f))$ には特異点が 1 つあり，極大イデアル $M = (2, x)$ である．M を中心とするブローアップ $y = x/2$ により，V は V' に変換される．V' の $\mathrm{Spec}(\mathbb{Z}[y])$ 上の定義式 $f' = 4y^4 - 2y^3 + y^2 - y + 1$ は特異点をもたないから，素数 2 は分岐しない．したがって，f の定める 4 次体においては $(2) = \mathfrak{P}_1\mathfrak{P}_2$ と分解し，点 $\mathfrak{P}_i$ の剰余体は $\mathbb{F}_4$ であることが分かる．この 4 次式は，ディリクレの『整数論講義』第 2 版 (1871) が出版されたときにデデキントが書いた広告にある例である．デデキントはこの 2 のように，判別式の重複因子のうちで分岐をしない因子を仮因子 (außerwesentlicher Diskriminantentheiler) とよんだが，仮因子は特異点と関係する．

1964 年当時の廣中の証明は，4 種類の解消データを用意して，次元に関する数学的帰納法により，順番に証明するという複雑なものであった．また，解消データを低次元のデータに帰着させるときにスキーム論の特徴である非閉点による局所化を用いたため，そのままでは複素解析空間の特異点解消には拡張できなかった．さらに，特異点の不変量が上半連続でなかったためブローアップの中心が具体的に記述できない，などの問題があった．

そこで廣中はいわゆる「庭園理論」を提唱し，特異点集合を土にたとえ，ブローアップの列による特異点の変換の列を森や林にたとえて，これらから特異点解消に必要な不変量を抽出することに成功した．この不変量は上半連続であるためブローアップすべき中心を具体的に教えてくれる．そのため，標数零の特異点解消の手順は格段に分かりやすくなった．

9. その後の発展

リーマン・ロッホの定理は代数幾何学以外の分野でも研究されている．一般のエクセレントスキームの特異点解消問題はまだ未解決であるが特異点の研究は盛んである．スキーム論以降の代数幾何学の発展については (2) に続く．

参考文献

1) A. Grothendieck et J. Dieudonné, *Élement de Géométrie Algébriques, I–IV. Publications Mathématiques IHES* (1960–1964).
2) R. Hartshorne（高橋宣能，松下大介訳），『代数幾何学 1,2,3』，丸善出版 (2004–2005).
3) 廣中平祐, Resolution of singularities of an algebraic variety over a field of characteristic zero, *Annals of Math.*, vol.**79**, 109–326 頁 (1964).
4) F. Hirzebruch（田中紀子訳），小平邦彦：数学者，我が友人，我が師，「数学の楽しみ」，No.**20**, 54–65 頁，日本評論社 (2000).
5) 岩澤健吉，『代数関数論』，岩波書店 (1954).
6) 小平邦彦, *Collected Works*, Vol.I, II, III, 岩波書店，プリンストン大学出版局 (1975).
7) 久保田富雄，古典 2 次形式に関する考察，『数論論説』，189–218 頁，牧野書店 (1999).
8) 向井茂，『モジュライ理論 1』，岩波書店 (1998).
9) J.-P. Serre, *Algèbre Locale Multiplicités*, Lecture Notes in Math. Vol.**11**, Springer (1965).
10) A. Speiser, Über die Komposition der binären quadratischen Formen, *Festschrift Heinrich Weber*, 375–395 頁，Teubner (1912).
11) O. Zariski, *Algebraic Surfaces*, Springer (1935).

（まえだ・ひろのぶ，東京農工大学大学院工学研究院）

特　集（2015年5月号予告）

物理と方程式

現象はいかに記述されるか

巻頭言	福嶋　健二
力学と方程式	浅田　秀樹
電磁気学の実験と方程式	岡部　洋一
相対性理論と方程式	郡　和範
量子力学と方程式	江藤　幹雄
流体力学と方程式	平野　哲文
スピンダイナミクスと方程式	多々良　源
素粒子の階層性と方程式	山脇　幸一
数理物理と方程式	笹本　智弘
[コラム]	高安　秀樹

特　集（2015年3月号）

団代数をめぐって

新たな共通構造の認識

団代数とは何か	中西　知樹
団代数ことはじめ	中西　知樹
団代数と傾理論，団傾理論	伊山　修
団代数と結晶基底	中島　俊樹
団代数と標準基底	木村　嘉之
団代数と Y システム	井上　玲
ミューテーションの分配級数	寺嶋　郁二
団代数と完全WKB解析	岩木　耕平
団代数と超対称ゲージ理論	山崎　雅人

《連載》	例題形式で探求する微積分学の基本定理	その14	森田　茂之
	例題形式で探求する代数学のエッセンス	その2	小林　正典
	経路積分と量子解析	その7	鈴木　増雄

編集後記

一昨年の4月号，昨年の3月号に続き，「○○における様々な発想」で特集を組ませていただきました．いかがでしたでしょうか．今回も代数独特の考え方が見て取れたのではないかと思います．

日頃，他の人が何を考えているのかを読み取ることは重要なことだと思います．それと同様に，学問の世界でもその分野ごとでどういう考え方がなされているのかを知ることは重要ではないでしょうか．時には問題解決のヒントになることもあると思います．本誌の特集がその一助になれば大変有り難いことです．　(R)

＊　　＊

小木曽先生の記事では代数学と幾何学が関連する代数幾何学について解説されています．そこで取り上げられている「円と直線はいつ交点をもつか」という問題をみて，大学受験の数学を思い出しました．式を図示することで考えやすくなり，問題を解くコツがわかってきて，きれいに解けたときの喜びや達成感が数学の面白さを知るきっかけとなりました．

昨年，一昨年と，幾何学，解析学の発想についても特集しました．3分野の関わりに着目して，それぞれを読み返してみるのも面白いのではと思います．　(T)

数　理　科　学　4月号

2015年4月1日発行

数理科学編集部　　　　発行人　木　下　敏　孝
TEL. (03) 5474–8816
FAX. (03) 5474–8817

ホームページ　http://www.saiensu.co.jp
ご意見・ご要望は　sk@saiensu.co.jp　まで．

発行所　©　株式会社 **サ イ エ ン ス 社**　　TEL. (03) 5474–8500 (代表)
〒151–0051 東京都渋谷区千駄ヶ谷1–3–25　振替 00170–7–2387　　(03) 5474–8600 (広告部)

印刷・製本　三美印刷株式会社　山岡景仁